Controlling Lightweight Access Points

This chapter contains these sections:

Access Point Communication Protocols

Information About Access Point Communication Protocols

Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate with the controller and other lightweight access points on the network.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is implemented in controller for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points can discover and join a CAPWAP controller, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

You can deploy CAPWAP controllers and LWAPP controllers on the same network. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exceptions are that the Cisco Aironet 1040, 1140, 1260, 3500, and 3600 Series Access Points, which support only CAPWAP and join only controllers that run CAPWAP. For example, an 1130 series access point can join a controller running either CAPWAP or LWAPP where an1140 series access point can join only a controller that runs CAPWAP.

The following are some guidelines that you must follow for access point communication protocols:

- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.
- Ensure that the CAPWAP UDP ports 5246 and 5247 (similar to the LWAPP UDP ports 12222 and 12223) are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- If access control lists (ACLs) are in the control path between the controller and its access points, you need to open new protocol ports to prevent access points from being stranded.

Restrictions for Access Point Communication Protocols

- On virtual controller platforms, per-client downstream rate limiting is not supported in FlexConnect central switching.
- Rate-limiting is applicable to all traffic destined to the CPU from either direction (wireless or wired). We recommend that you always run the controller with the default **config advanced rate enable** command in effect to rate limit traffic to the controller and protect against denial-of-service (DoS) attacks. You can use the **config advanced rate disable** command to stop rate-limiting of Internet Control Message Protocol (ICMP) echo responses for testing purposes. However, we recommend that you reapply the **config advanced rate enable** command after testing is complete.
- Ensure that the controllers are configured with the correct date and time. If the date and time configured on the controller precedes the creation and installation date of certificates on the access points, the access point fails to join the controller.

Configuring Data Encryption

Cisco 5500 Series Controllers enable you to encrypt CAPWAP control packets (and optionally, CAPWAP data packets) that are sent between the access point and the controller using Datagram Transport Layer Security (DTLS). DTLS is a standards-track Internet Engineering Task Force (IETF) protocol based on TLS. CAPWAP control packets are management packets exchanged between a controller and an access point while CAPWAP data packets encapsulate forwarded wireless frames. CAPWAP control and data packets are sent over separate UDP ports: 5246 (control) and 5247 (data). If an access point does not support DTLS data encryption, DTLS is enabled only for the control plane, and a DTLS session for the data plane is not established.

Note With Release 8.2, DTLSv1.2 for CAPWAP is not supported. The following are supported for web authentication and WebAdmin based on the configuration:

- TLSv1.2
- TLSv1.0
- SSLv3
- SSLv2

Note Cisco WLC supports only static configuration of gateway. Therefore, the ICMP redirect to change IP address of the gateway is not considered.

Guidelines for Data Encryption

- Cisco 1130 and 1240 series access points support DTLS data encryption with software-based encryption.
- Cisco 1040, 1140, 1250, 1260, 1530, 1550, 1600, 1700, 2600, 2700, 3500, 3600, and 3700 series access points support DTLS data encryption with hardware-based encryption

- Cisco Aironet 1552 and 1522 outdoor access points support data DTLS.
- DTLS data encryption is not supported on Cisco Aironet 700 Series Access Points.
- DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points. Most access points are deployed in a secure network within a company building, so data encryption is not necessary. In contrast, the traffic between an OfficeExtend access point and the controller travels through an unsecure public network, so data encryption is more important for these access points. When data encryption is enabled, traffic is encrypted at the access point before it is sent to the controller and at the controller before it is sent to the client.
- Encryption limits throughput at both the controller and the access point, and maximum throughput is desired for most enterprise networks.
- In a Cisco unified local wireless network environment, do not enable DTLS on the Cisco 1130 and 1240 access points, as it may result in severe throughput degradation and may render the APs unusable.

  See the OfficeExtend Access Points section for more information on OfficeExtend access points.
- You can use the controller to enable or disable DTLS data encryption for a specific access point or for all access points.
- The availability of data DTLS is as follows:
  - The Cisco 5500 Series Controller will be available with two licenses options: One that allows data DTLS without any license requirements and another image that requires a license to use data DTLS. See the Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers section. The images for the DTLS and licensed DTLS images are as follows:

    Licensed DTLS—AS_5500_LDPE_x_x_x_x.aes

    Non licensed DTLS—AS_5500_x_x_x_x.aes
  - Cisco 2500, Cisco WiSM2—By default, these platforms do not contain DTLS. To turn on data DTLS, you must install a license. These platforms have a single image with data DTLS turned off. To use data DTLS you must have a license.
- If your controller does not have a data DTLS license and if the access point associated with the controller has DTLS enabled, the data path will be unencrypted.
- Non-Russian customers using Cisco 5508 Series Controller do not need data DTLS license. However all customers using Cisco 2500 Series Controllers, Cisco 8500 Series Controllers, WISM2, and need a data DTLS license to turn on the Data DTLS feature.

Upgrading or Downgrading DTLS Images for Cisco 5500 Series Controllers

Step 1 The upgrade operation fails on the first attempt with a warning indicating that the upgrade to a licensed DTLS image is irreversible.

Note Do not reboot the controller after Step 1.

Step 2 On a subsequent attempt, the license is applied and the image is successfully updated.

Guidelines When Upgrading to or from a DTLS Image

- You cannot install a regular image (nonlicensed data DTLS) once a licensed data DTLS image is installed.
- You can upgrade from one licensed DTLS image to another licensed DTLS image.
- You can upgrade from a regular image (DTLS) to a licensed DTLS image in a two step process.
- You can use the **show sysinfo** command to verify the LDPE image, before and after the image upgrade.

Configuring Data Encryption (GUI)

Ensure that the base license is installed on the Cisco 5500 Series Controller. Once the license is installed, you can enable data encryption for the access points.

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to enable data encryption.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 4 Select the **Data Encryption** check box to enable data encryption for this access point or unselect it to disable this feature. The default value is unselected.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 5 Click **Apply**.

Step 6 Click **Save Configuration**.

Configuring Data Encryption (CLI)

Note In images without a DTLS license, the **config** or **show** commands are not available.

To enable DTLS data encryption for access points on the controller using the controller CLI, follow these steps:

Step 1 Enable or disable data encryption for all access points or a specific access point by entering this command: **config ap link-encryption** {**enable** | **disable**} {**all** | *Cisco_AP*}

The default value is disabled.

Note Changing the data encryption mode requires the access points to rejoin the controller.

Step 2 When prompted to confirm that you want to disconnect the access point(s) and attached client(s), enter **Y**.

Step 3 Enter the **save config** command to save your configuration.

Step 4 See the encryption state of all access points or a specific access point by entering this command:

show ap link-encryption {**all** | *Cisco_AP*}

This command also shows authentication errors, which tracks the number of integrity check failures, and replay errors, which tracks the number of times that the access point receives the same packet.

Step 5 See a summary of all active DTLS connections by entering this command:
show dtls connections

Note If you experience any problems with DTLS data encryption, enter the **debug dtls** {**all** | **event** | **trace** | **packet**} {**enable** | **disable**} command to debug all DTLS messages, events, traces, or packets.

Viewing CAPWAP Maximum Transmission Unit Information

See the maximum transmission unit (MTU) for the CAPWAP path on the controller by entering this command:

show ap config general *Cisco_AP*

The MTU specifies the maximum size of any packet (in bytes) in a transmission.

Information similar to the following appears:

```
Cisco AP Identifier.............................. 9
Cisco AP Name.................................... Maria-1250
Country code..................................... US  - United States
Regulatory Domain allowed by Country............. 802.11bg:-A     802.11a:-A
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... 00:1f:ca:bd:bc:7c
IP Address Configuration......................... DHCP
IP Address....................................... 1.100.163.193
IP NetMask....................................... 255.255.255.0
CAPWAP Path MTU.................................. 1485
```

Debugging CAPWAP

Use these commands to obtain CAPWAP debug information:

- **debug capwap events** {**enable** | **disable**}—Enables or disables debugging of CAPWAP events.
- **debug capwap errors** {**enable** | **disable**}—Enables or disables debugging of CAPWAP errors.
- **debug capwap detail** {**enable** | **disable**}—Enables or disables debugging of CAPWAP details.
- **debug capwap info** {**enable** | **disable**}—Enables or disables debugging of CAPWAP information.
- **debug capwap packet** {**enable** | **disable**}—Enables or disables debugging of CAPWAP packets.
- **debug capwap payload** {**enable** | **disable**}—Enables or disables debugging of CAPWAP payloads.
- **debug capwap hexdump** {**enable** | **disable**}—Enables or disables debugging of the CAPWAP hexadecimal dump.
- **debug capwap dtls-keepalive** {**enable** | **disable**}—Enables or disables debugging of CAPWAP DTLS data keepalive packets.

Controller Discovery Process

In a CAPWAP environment, a lightweight access point discovers a controller by using CAPWAP discovery mechanisms and then sends the controller a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

The following are some guidelines for the controller discovery process:

- Upgrade and downgrade paths from LWAPP to CAPWAP or from CAPWAP to LWAPP are supported. An access point with an LWAPP image starts the discovery process in LWAPP. If it finds an LWAPP controller, it starts the LWAPP discovery process to join the controller. If it does not find a LWAPP controller, it starts the discovery in CAPWAP. If the number of times that the discovery process starts with one discovery type (CAPWAP or LWAPP) exceeds the maximum discovery count and the access point does not receive a discovery response, the discovery type changes to the other type. For example, if the access point does not discover the controller in LWAPP, it starts the discovery process in CAPWAP.
- If an access point is in the UP state and its IP address changes, the access point tears down the existing CAPWAP tunnel and rejoins the controller.
- To configure the IP addresses that the controller sends in its CAPWAP discovery responses, use the **config network ap-discovery nat-ip-only** {**enable** | **disable**} command.
- Access points must be discovered by a controller before they can become an active part of the network. The lightweight access points support the following controller discovery processes:
  - Layer 3 CAPWAP or LWAPP discovery—This feature can be enabled on different subnets from the access point and uses either IPv4 or IPv6 addresses and UDP packets rather the MAC addresses used by Layer 2 discovery.
  - CAPWAP Multicast Discovery—Broadcast does not exist in IPv6 address. Access point sends CAPWAP discovery message to all the controllers multicast address (FF01::18C). The controller receives the IPv6 discovery request from the AP only if it is in the same L2 segment and sends back the IPv6 discovery response.
  - Locally stored controller IPv4 or IPv6 address discovery—If the access point was previously associated to a controller, the IPv4 or IPv6 addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IPv4 or IPv6 addresses on an access point for later deployment is called *priming the access point*.
  - DHCP server discovery using option 43—This feature uses DHCP option 43 to provide controller IPv4 addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the Using DHCP Option 43 and DHCP Option 60 section.
  - DHCP server discovery using option 52 —This feature uses DHCP option 52 to allow the AP to discover the IPv6 address of the controller to which it connects. As part of the DHCPv6 messages, the DHCP server provides the controllers management with an IPv6 address.
  - DNS discovery—The access point can discover controllers through your domain name server (DNS). You must configure your DNS to return controller IPv4 and IPv6 addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name.

    When an access point receives an IPv4/IPv6 address and DNSv4/DNSv6 information from a DHCPv4/DHCPv6 server, it contacts the DNS to resolve

CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, which may include either IPv4 addresses or IPv6 addresses or both the addresses, the access point sends discovery requests to the controllers.

Restrictions for Controller Discovery Process

- During the discovery process, the 1040, 1140, 1260, 3500, and 3600 series access points will only query for Cisco CAPWAP Controllers. It will not query for LWAPP controllers. If you want these access points to query for both LWAPP and CAPWAP controllers then you need to update the DNS.
- Ensure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.
- To avoid downtime restart CAPWAP on AP while configuring Global HA , so that AP goes back and joins the backup primary controller. This starts a discovery with the primary controller in the back ground. If the discovery with primary is successful, it goes back and joins the primary again.

Verifying that Access Points Join the Controller

When replacing a controller, ensure that access points join the new controller.

Verifying that Access Points Join the Controller (GUI)

Step 1 Configure the new controller as a master controller as follows:
a) Choose **Controller** > **Advanced** > **Master Controller Mode** to open the Master Controller Configuration page.
b) Select the **Master Controller Mode** check box.
c) Click **Apply** to commit your changes.
d) Click **Save Configuration** to save your changes.

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure.

Step 3 Restart the access points.

Step 4 Once all the access points have joined the new controller, configure the controller not to be a master controller by unselecting the **Master Controller Mode** check box on the Master Controller Configuration page.

Verifying that Access Points Join the Controller (CLI)

Step 1 Configure the new controller as a master controller by entering this command:

config network master-base enable

Step 2 (Optional) Flush the ARP and MAC address tables within the network infrastructure.

Step 3 Restart the access points.

Step 4 Configure the controller not to be a master controller after all the access points have joined the new controller by entering this command:
config network master-base disable

Searching for Access Points

Information About Searching for Access Points

You can search for specific access points in the list of access points on the All APs page. To do so, you create a filter to display only access points that meet certain criteria (such as MAC address, status, access point mode, and certificate type). This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

Searching the AP Filter (GUI)

Step 1 Choose **Monitor** > **Access Point Summary**> **All APs** > **Details** to open the All APs page.
This page lists all of the access points joined to the controller. For each access point, you can see its name, MAC address, uptime, status, operating mode, certificates, OfficeExtend access point status, and access point submode.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 20 access points.

Step 2 Click **Change Filter** to open the Search AP dialog box.

Step 3 Select one or more of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address—**The MAC address of an access point.

  Note When you enable the MAC Address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC Address filter is disabled automatically.

- **AP Name—**Enter the name of an access point.
- **AP Model—**Enter the model name of an access point.
- **Operating Status—**Select one or more of the following check boxes to specify the operating status of the access points:
  - **UP—**The access point is up and running.

    Note When the APs are in downloading state, during which time the APs are nonfunctional due to no configuration on the APs, the WLC GUI shows these AP radios in UP state on the Monitor page.

- **DOWN—**The access point is not operational.
- **REG—**The access point is registered to the controller.
- **DEREG—**The access point is not registered to the controller.
- **DOWNLOAD—**The controller is downloading its software image to the access point.

- **Port Number—**Enter the controller port number to which the access point is connected.
- **Admin Status—**Choose **Enabled** or **Disabled** to specify whether the access points are enabled or disabled on the controller.
- **AP Mode—**Select one or more of the following options to specify the operating mode of the access points:
  - **Local—The default option.**

    Note The 600 OEAP series access point uses only local mode.

    When an access point in local mode connects to a Cisco Flex 7500 Series Controller, it does not serve clients. The access point details are available in the controller. To enable an access point to serve clients or perform monitoring-related tasks when connected to the Cisco Flex 7500 Series Controller, the access point mode must be in FlexConnect or monitor mode. Use the following command to automatically convert access points to a FlexConnect mode or monitor mode on joining the controller:

    config ap autoconvert {**flexconnect** | **monitor** | **disable**}

    All access points that connect to the controller will either be converted to FlexConnect mode or monitor mode depending on the configuration provided.
  - **FlexConnect—**This mode is used for 1040, 1130, 1140, 1240, 1250, 1260, 1600, 2600, 3500, 3600, and 800 access points.
  - **REAP—**This mode is the remote edge lightweight access point.
  - **Monitor—**This mode is the monitor-only mode.
  - **Rogue Detector—**This mode monitors the rogue APs on wire. It does not transmit or receive frames over the air or contain rogue APs.

    Note Information about rogues that are detected is not shared between controllers. Therefore, we recommend that every controller has its own connected rogue detector AP when rogue detector APs are used.
  - **Sniffer—**The access point starts sniffing the air on a given channel. It captures and forwards all the packets from the clients on that channel to a remote machine that runs Airopeek or Wireshark (packet analyzers for IEEE 802.11 wireless LANs). It includes information on the time stamp, signal strength, packet size, and so on.

    Note The Bridge option is displayed only if the AP is bridge capable.

    Note If the AP mode is set to “Bridge” and the AP is not REAP capable, an error appears.

    Note In the access point sniffer, the server to which the data is to be sent should be on the same VLAN as the wireless controller management VLAN otherwise an error will be displayed.
  - **Bridge—**This mode sets the AP mode to “Bridge” if you are connecting a Root AP.

- **SE-Connect—**This mode allows you to connect to spectrum expert and it allows the access point to perform spectrum intelligence.

  Note Spectrum intelligence is supported on , 2600 and 3600 series access points. 1260 series access points does not support the spectrum intelligence.

  Note When an access point is configured in SE-Connect mode, the access point reboots and rejoins the controller. Access points that are configured in this mode do not serve the client.

- **Flex+Bridge—** The standalone mode support is applicable when the AP is in this mode.

- **Certificate Type—**Select one or more of the following check boxes to specify the types of certificates installed on the access points:
  - **MIC—**Manufactured-installed certificate
  - **SSC—**Self-signed certificate
  - **LSC—**Local significant certificate

  Note See the Authorizing Access Points section for more information about these certificate types.

- **Primary S/W Version—**Select this check box to enter the primary software version number
- **Backup S/W Version—**Select this check box to enter the secondary software version number.

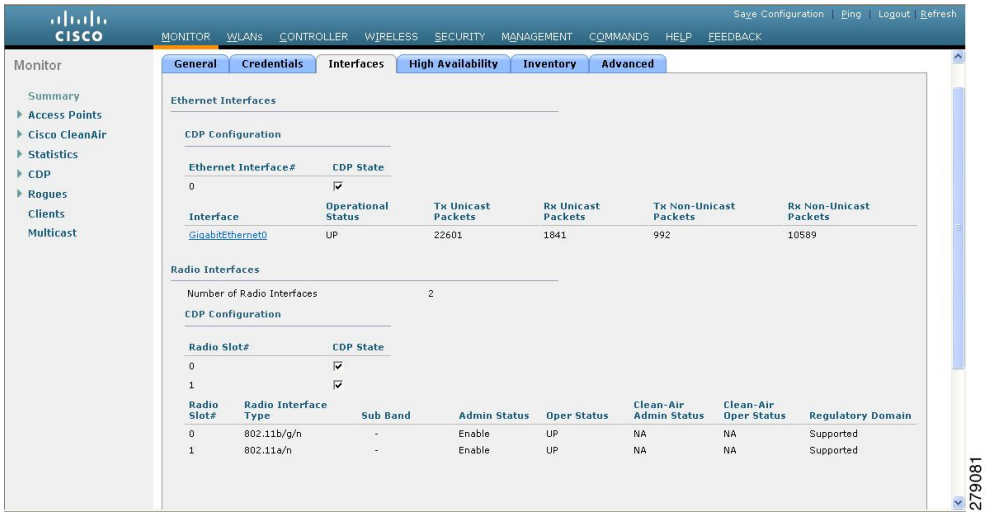
Step 4 Click **Apply**.
Only the access points that match your search criteria appear on the All APs page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1d:e5:54:0e:e6, AP Name:pmsk-ap, Operational Status: UP, Status: Enabled, and so on).
Note If you want to remove the filters and display the entire access point list, click **Clear Filter**.

Monitoring the Interface Details

Step 1 Choose **Monitor** > **Summary** > **All APs**. The All APs > Details page appears.

Step 2 Click the **Interfaces** tab.

Figure 1: Interfaces Tab



Step 3 Click on the available Interface name. The Interface Details page appears.

Step 4 The Interface Details page displays the following parameter details.

Table 1: Interfaces Parameters Details

Button	Description
AP Name	Name of the access point.
Link Speed	Speed of the interference in Mbps.
RX Bytes	Total number of bytes in the error-free packets received on the interface.
RX Unicast Packets	Total number of unicast packets received on the interface.
RX Non-Unicast Packets	Total number of nonunicast or multicast packets received on the interface.
Input CRC	Total number of CRC error in packets while receiving on the interface.
Input Errors	Sum of all errors in the packets while receiving on the interface.

Button	Description
Input Overrun	Number of times the receiver hardware was incapable of handling received data to a hardware buffer because the input rate exceeded the receiver's capability to handle that data.
Input Resource	Total number of resource errors in packets received on the interface.
Runts	Number of packets that are discarded because they are similar to the medium's minimum packet size.
Throttle	Total number of times the interface advised a sending NIC that it was overwhelmed by packets being sent and to slow the pace of delivery.
Output Collision	Total number of packet retransmitted due to an Ethernet collision.
Output Resource	Resource errors in packets transmitted on the interface.
Output Errors	Errors that prevented the final transmission of packets out of the interface.
Operational Status	Operational state of the physical ethernet interface on the AP.
Duplex	Interface's duplex mode.
TX Bytes	Number of bytes in the error-free packets transmitted on the interface.
TX Unicast Packets	Total number of unicast packets transmitted on the interface.
TX Non-Unicast Packets	Total number of nonunicast or multicast packets transmitted on the interface.
Input Aborts	Total number of packets aborted while receiving on the interface.
Input Frames	Total number of packets received incorrectly that has a CRC error and a noninteger number of octets on the interface.
Input Drops	Total number of packets dropped while receiving on the interface because the queue was full.
Unknown Protocol	Total number of packets discarded on the interface due to an unknown protocol.
Giants	Number of packets that are discarded because they exceeded the medium's maximum packet size.
Interface Resets	Number of times that an interface has been completely reset.
Output No Buffer	Total number of packets discarded because there was no buffer space.
Output Underrun	Number of times the transmitter has been running faster than the router can handle.

Button	Description
Output Total Drops	Total number of packets dropped while transmitting from the interface because the queue was full.

Searching for Access Point Radios

Information About Searching for Access Point Radios

You can search for specific access point radios in the list of radios on the 802.11a/n Radios page or the 802.11b/g/n Radios page. You can access these pages from the Monitor tab on the menu bar when viewing access point radios or from the Wireless tab on the menu bar when configuring access point radios. To search for specific access point radios, you create a filter to display only radios that meet certain criteria (such as radio MAC address, access point name, or CleanAir status). This feature is especially useful if your list of access point radios spans multiple pages, which prevents you from viewing them all at once.

Searching for Access Point Radios (GUI)

Step 1 Perform either of the following:

- Choose **Monitor** > **Access Points Summary** > **802.11a/n (or 802.11b/g/n)** > **Radios** > **Details** to open the 802.11a/n (or 802.11b/g/n) Radios page.
- Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n** (or **802.11b/g/n**) to open the 802.11a/n (or 802.11b/g/n) Radios page.

  These pages show all of the 802.11a/n or 802.11b/g/n access point radios that are joined to the controller and their current settings.

  The total number of access point radios appears in the upper right-hand corner of the page. If the list of radios spans multiple pages, you can access these pages by clicking the page number links. Each page shows up to 25 access point radios.

  Note In a Cisco Unified Wireless Network environment, the 802.11a/n and 802.11b/g/n radios should not be differentiated based on their Base Radio MAC addresses, as they may have the same addresses. Instead, the radios should be differentiated based on their physical addresses.

Step 2 Click **Change Filter** to open the **Search AP** dialog box.

Step 3 Select one of the following check boxes to specify the criteria used when displaying access point radios:

- **MAC Address—**Base radio MAC address of an access point radio.

- **AP Name—**Access point name.

  Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **CleanAir Status—**Select one or more of the following check boxes to specify the operating status of the access points:
  - **UP—**The spectrum sensor for the access point radio is currently operational.
  - **DOWN—**The spectrum sensor for the access point radio is currently not operational because an error has occurred. The most likely reason for the error is that the access point radio is disabled.
  - **ERROR—**The spectrum sensor for the access point radio has crashed, making CleanAir monitoring nonoperational for this radio. We recommend rebooting the access point or disabling CleanAir functionality on the radio.
  - **N/A—**The access point radio is not capable of supporting CleanAir functionality. Currently, only Cisco Aironet 3500 series access point radios can be configured for Cisco CleanAir.

Step 4 Click **Find** to commit your changes. Only the access point radios that match your search criteria appear on the 802.11a/n Radios page or the 802.11b/g/n Radios page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point radio list, click **Clear Filter**.

Configuring Global Credentials for Access Points

Information About Configuring Global Credentials for Access Points

Cisco IOS access points are shipped from the factory with *Cisco* as the default enable password. This password allows users to log onto the nonprivileged mode and enter **show** and **debug** commands, which poses a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to enter configuration commands from the access point's console port.

The following are some guidelines to configure global credentials for access points:

- You can set a global username, password, and enable password that all access points that are currently joined to the controller and any that join in the future inherit as they join the controller. If desired, you can override the global credentials and assign a unique username, password, and enable password for a specific access point.
- After an access point joins the controller, the access point enables console port security, and you are prompted for your username and password whenever you log into the access point's console port. When you log on, you are in nonprivileged mode, and you must enter the enable password in order to use the privileged mode.

- The global credentials that you configure on the controller are retained across controller and access point reboots. They are overwritten only if the access point joins a new controller that is configured with a global username and password. If the new controller is not configured with global credentials, the access point retains the global username and password configured for the first controller.
- You must keep track of the credentials used by the access points. Otherwise, you might not be able to log onto the console port of the access point. If you need to return the access points to the default *Cisco*/*Cisco* username and password, you must clear the controller's configuration and the access point's configuration to return them to factory-default settings. To clear the controller's configuration, choose **Commands** > **Reset to Factory Default** > **Reset** on the controller GUI, or enter the **clear config** command on the controller CLI. To clear the access point's configuration, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear All Config** on the controller GUI, or enter the **clear ap config** *Cisco_AP* command on the controller CLI. To clear the access point's configuration except its static IP address, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Clear Config Except Static IP**, or enter the **clear ap config** *ap-name* **keep-ip-config** command on the controller CLI. After the access point rejoins a controller, it adopts the default *Cisco*/*Cisco* username and password.

Note Suppose you configure an indoor Cisco AP to go into the mesh mode. If you want to reset the Cisco AP to the local mode, use the **test mesh mode local** command.

- To reset the AP hardware, choose **Wireless** > **Access Points** > **All APs**, click the AP name and click **Reset AP Now**.

Restrictions for Global Credentials for Access Points

- The controller software features are supported on all access points that have been converted to lightweight mode except the 1100 series. VxWorks access points are not supported.
- Telnet is not supported on Cisco Aironet 1830 and 1850 Series Access Points.

Configuring Global Credentials for Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 3 In the Password text box, enter the password that is to be inherited by all access points that join the controller.
You can set a global username, password, and enable password that all access points inherit as they join the controller including access points that are currently joined to the controller and any that join in the future. You can override the global credentials and assign a unique username, password, and enable password for a specific access point. The following are requirements enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.

- The password should not contain the management username or the reverse of the username.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

Step 4 In the Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller.

Step 5 Click **Apply** to send the global username, password, and enable password to all access points that are currently joined to the controller or that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

Step 7 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to override the global credentials.
c) Choose the **Credentials** tab. The All APs > Details for (Credentials) page appears.
d) Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.
e) In the Username, Password, and Enable Password text boxes, enter the unique username, password, and enable password that you want to assign to this access point.
Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.
f) Click **Apply** to commit your changes.
g) Click **Save Configuration** to save your changes.
Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Configuring Global Credentials for Access Points (CLI)

Step 1 Configure the global username, password, and enable password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:
config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password* **all**

Step 2 (Optional) Override the global credentials for a specific access point and assign a unique username, password, and enable password to this access point by entering this command:
config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*
The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

Step 3 Enter the **save config** command to save your changes.

Step 4 Verify that global credentials are configured for all access points that join the controller by entering this command:

show ap summary

Note If global credentials are not configured, the Global AP User Name text box shows "Not Configured."

To view summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

Step 5 See the global credentials configuration for a specific access point by entering this command:
show ap config general *Cisco_AP*

Note The name of the access point is case sensitive.

Note If this access point is configured for global credentials, the AP User Mode text boxes shows "Automatic." If the global credentials have been overwritten for this access point, the AP User Mode text box shows "Customized."

Configuring Authentication for Access Points

Information About Configuring Authentication for Access Points

You can configure 802.1X authentication between a lightweight access point and a Cisco switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

You can configure global authentication settings that all access points that are currently associated with the controller and any that associate in the future. You can also override the global authentication settings and assign unique authentication settings for a specific access point.

Restrictions for Authenticating Access Points

- The OEAP 600 Series access points do not support LEAP.
- The Bridge Protocol Data Unit (BPDU) guard should always be disabled on the switch port connected to the AP. Enabling of BPDU guard is allowed only when the switch puts the port in port fast mode.

Prerequisites for Configuring Authentication for Access Points

Step 1 If the access point is new, do the following:

a) Boot the access point with the installed recovery image.

b) If you choose not to follow this suggested flow and instead enable 802.1X authentication on the switch port connected to the access point prior to the access point joining the controller, enter this command:
lwapp ap dot1x username *username* **password** *password*

Note If you choose to follow this suggested flow and enable 802.1X authentication on the switch port after the access point has joined the controller and received the configured 802.1X credentials, you do not need to enter this command.

Note This command is available only for access points that are running the 5.1, 5.2, 6.0, or 7.0 recovery image.

Connect the access point to the switch port.

Step 2 Install the 5.1, 5.2, 6.0, or 7.0 image on the controller and reboot the controller.

Step 3 Allow all access points to join the controller.

Step 4 Configure authentication on the controller. See the Configuring Authentication for Access Points (GUI) section or the Configuring Authentication for Access Points (CLI) section for information about configuring authentication on the controller.

Step 5 Configure the switch to allow authentication. See the Configuring the Switch for Authentication section for information about configuring the switch for authentication.

Configuring Authentication for Access Points

Configuring Authentication for Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 Under 802.1x Supplicant Credentials, select the **802.1x Authentication** check box.

Step 3 In the Username text box, enter the username that is to be inherited by all access points that join the controller.

Step 4 In the Password and Confirm Password text boxes, enter the password that is to be inherited by all access points that join the controller.

Note You must enter a strong password in these text boxes. Strong passwords have the following characteristics:

- They are at least eight characters long
- They contain a combination of uppercase and lowercase letters, numbers, and symbols
- They are not a word in any language

Step 5 Click **Apply** to send the global authentication username and password to all access points that are currently joined to the controller and to any that join the controller in the future.

Step 6 Click **Save Configuration** to save your changes.

Step 7 If desired, you can choose to override the global authentication settings and assign a unique username and password to a specific access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to override the authentication settings.
c) Click the **Credentials** tab to open the All APs > Details for (Credentials) page.
d) Under 802.1x Supplicant Credentials, select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global authentication username and password from the controller. The default value is unselected.

e) In the Username, Password, and Confirm Password text boxes, enter the unique username and password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and whenever the access point joins a new controller.

f) Click **Apply** to commit your changes.

g) Click **Save Configuration** to save your changes.

Note If you want to force this access point to use the controller's global authentication settings, unselect the **Over-ride Global Credentials** check box.

Configuring Authentication for Access Points (CLI)

Step 1 Configure the global authentication username and password for all access points currently joined to the controller as well as any access points that join the controller in the future by entering this command:
config ap 802.1Xuser add username *ap-username* **password** *ap-password* **all**

Note You must enter a strong password for the *ap-password* parameter. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

Step 2 (Optional) Override the global authentication settings and assign a unique username and password to a specific access point. To do so, enter this command:
config ap 802.1Xuser add username *ap-username* **password** *ap-password Cisco_AP*

Note You must enter a strong password for the *ap-password* parameter. See the note in Step 1 for the characteristics of strong passwords.

The authentication settings that you enter in this command are retained across controller and access point reboots and whenever the access point joins a new controller.

Note If you want to force this access point to use the controller's global authentication settings, enter the **config ap 802.1Xuser delete** *Cisco_AP* command. The following message appears after you execute this command: "`AP reverted to global username configuration.`"

Step 3 Enter the **save config** command to save your changes.

Step 4 (Optional) Disable 802.1X authentication for all access points or for a specific access point by entering this command:
config ap 802.1Xuser disable {**all** | *Cisco_AP*}

Note You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

Step 5 See the authentication settings for all access points that join the controller by entering this command:
show ap summary

Information similar to the following appears:

```
Number of APs.................................. 1
Global AP User Name............................ globalap
Global AP Dot1x User Name...................... globalDot1x
```

Step 6 See the authentication settings for a specific access point by entering this command: **show ap config general** *Cisco_AP*

Note The name of the access point is case sensitive.

Note If this access point is configured for global authentication, the AP Dot1x User Mode text boxes shows "Automatic." If the global authentication settings have been overwritten for this access point, the AP Dot1x User Mode text box shows "Customized."

Configuring the Switch for Authentication

To enable 802.1X authentication on a switch port, on the switch CLI, enter these commands:

- Switch# **configure terminal**
- Switch(config)# **dot1x system-auth-control**
- Switch(config)# **aaa new-model**
- Switch(config)# **aaa authentication dot1x default group radius**
- Switch(config)# **radius-server host** *ip_addr* **auth-port** *port* **acct-port** *port* **key** *key*
- Switch(config)# **interface fastethernet2/1**
- Switch(config-if)# **switchport mode access**
- Switch(config-if)# **dot1x pae authenticator**
- Switch(config-if)# **dot1x port-control auto**
- Switch(config-if)# **end**

Configuring Embedded Access Points

Information About Embedded Access Points

Controller software release 7.0.116.0 or later releases support the embedded access points: AP801 and AP802, which are the integrated access points on the Cisco 880 Series Integrated Services Routers (ISRs). This access points use a Cisco IOS software image that is separate from the router Cisco IOS software image. The access points can operate as autonomous access points configured and managed locally, or they can operate as

centrally managed access points that utilize the CAPWAP or LWAPP protocol. The AP801 and AP802 access points are preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.

The following are some guidelines for embedded access points:

- Before you use an AP801 or AP802 Series Lightweight Access Point with controller software release 7.0.116.0 or later releases, you must upgrade the software in the Next Generation Cisco 880 Series Integrated Services Routers (ISRs) to Cisco IOS 151-4.M or later.

  Note In Release 7.4, all AP modes except bridging (required for mesh) are supported for both AP801 and AP802. In Release 7.5 and later, all AP modes are supported on AP802; however, bridging is not supported on AP801.

- When you want to use the AP801 or AP802 with a controller, you must enable the recovery image for the unified mode on the access point by entering the **service-module wlan-ap 0 bootimage unified** command on the router in privileged EXEC mode.
- If the **service-module wlan-ap 0 bootimage unified** command does not work, make sure that the software license is still eligible.
- After enabling the recovery image, enter the **service-module wlan-ap 0 reload** command on the router to shut down and reboot the access point. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.

  Note To use the CLI commands mentioned above, the router must be running Cisco IOS Release 12.4(20)T or later releases.

- To support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this Cisco IOS image on the router. For licensing information, see http://www.cisco.com/c/en/us/td/docs/routers/access/sw_activation/SA_on_ISR.html.
- After the AP801 or AP802 boots up with the recovery image for the unified mode, it requires an IP address to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task:

  ip dhcp pool *pool_name*

  network *ip_address subnet_mask*

  dns-server *ip_address*

  default-router *ip_address*

  option 43 hex *controller_ip_address_in_hex*

  Example:

```
ip dhcp pool embedded-ap-pool
 network 60.0.0.0 255.255.255.0
   dns-server 171.70.168.183
   default-router 60.0.0.1
   option 43 hex  f104.0a0a.0a0f   /* single WLC IP address(10.10.10.15) in hex format
```

*/

- The AP801 and AP802 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 and AP802 access points store the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user's configuration.
- The AP801 and AP802 access points can be used in FlexConnect mode.

For more information about the AP801, see the documentation for the Cisco 800 Series ISRs at http://www.cisco.com/c/en/us/support/routers/800-series-routers/tsd-products-support-series-home.html.

For more information about the AP802, see the documentation for the Next generation Cisco 880 Series ISRs at http://www.cisco.com/c/dam/en/us/td/docs/routers/access/800/860-880-890/software/configuration/guide/SCG_880_series.pdf.

Converting Autonomous Access Points to Lightweight Mode

Information About Converting Autonomous Access Points to Lightweight Mode

You can convert any autonomous mode Cisco Aironet access point, to lightweight mode. When you upgrade one of these access points to lightweight mode, the access point communicates with a controller and receives a configuration and software image from the controller.

See the Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode document for instructions to upgrade an autonomous access point to lightweight mode:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01101010.html

The following are some guidelines for converting autonomous APs to lightweight mode APs:

- All Cisco lightweight access points support 16 BSSIDs per radio and a total of 16 wireless LANs per access point. When a converted access point associates with a controller, wireless LANs with IDs 1 through 16 are pushed to the access point if the AP is part of the default AP group on the controller. You can use other AP group configurations to push other wireless LANs to the new AP.

  When a 802.11ac module (the RM3000AC) is added to a 3600 AP, you can have only 8 wireless LANs on the 802.11a/n/ac radio.
- Access points converted to lightweight mode must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.

Restrictions for Converting Autonomous Access Points to Lightweight Mode

- Access points converted to lightweight mode do not support Wireless Domain Services (WDS). Converted access points communicate only with Cisco wireless LAN controllers and cannot communicate with WDS devices. However, the controller provides functionality that is equivalent to WDS when the access point associates to it.
- After you convert an access point to lightweight mode, the console port provides read-only access to the unit.

Reverting from Lightweight Mode to Autonomous Mode

After you convert an autonomous access point to lightweight mode, you can convert the access point from a lightweight unit back to an autonomous unit by loading a Cisco IOS release that supports autonomous mode. If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP. In either method, the access point must be able to access a TFTP server that contains the Cisco IOS release to be loaded.

Reverting to a Previous Release (CLI)

Step 1 Log on to the CLI on the controller to which the access point is associated.

Step 2 Revert from lightweight mode, by entering this command:
config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*

Step 3 Wait until the access point reboots and reconfigure the access point using the CLI or GUI.

Reverting to a Previous Release Using the MODE Button and a TFTP Server

Step 1 Configure the PC on which your TFTP server software runs with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *ap3g2-k9w7-tar.152-4.JB4.tar* for a 2700 or 3700 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to **ap3g2-k9w7-tar.default** for a 2700 or a 3700 series access point.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Note The MODE button on the access point must be enabled. Follow the steps in the Disabling the Reset Button on Access Points Converted to Lightweight Mode to select the status of the access point MODE button.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure the access point using the GUI or the CLI.

Authorizing Access Points

In controller software releases prior to 5.2, the controller may either use self-signed certificates (SSCs) to authenticate access points or send the authorization information to a RADIUS server (if access points have

manufactured-installed certificates [MICs]). In controller software release 5.2 or later releases, you can configure the controller to use a local significant certificate (LSC).

Access points manufactured after July 18, 2005 contain a manufactured-installed certificate (MIC). The controller can use this certificate to authenticate the access points. Alternatively, you can use an authentication list on the controller or an external RADIUS server.

Authorizing Access Points Using SSCs

The Control and Provisioning of Wireless Access Points protocol (CAPWAP) secures the control communication between the access point and controller by a secure key distribution requiring X.509 certificates on both the access point and controller. CAPWAP relies on provisioning of the X.509 certificates. Cisco Aironet access points shipped before July 18, 2005 do not have a MIC, so these access points create an SSC when upgraded to operate in lightweight mode. Controllers are programmed to accept local SSCs for authentication of specific access points and do not forward those authentication requests to a RADIUS server. This behavior is acceptable and secure.

Authorizing Access Points for Virtual Controllers Using SSC

Virtual controllers use SSC certificates instead of Manufacturing Installed Certificates (MIC) used by physical controllers. You can configure the controller to allow an AP to validate the SSC of the virtual controller. When an AP validates the SSC, the AP checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the AP associates with the controller. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. An AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC, the AP bypasses the hash validation and directly moves to the Run state. APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated with a physical controller and hash validation is disabled, the AP associates with any virtual controller without hash validation. The hash key of the virtual controller can be configured for a mobility group member. This hash key gets pushed to the APs, so that the APs can validate the hash key of the controller.

Configuring SSC (GUI)

Step 1 Choose **Security** > **Certificate** > **SSC** to open the Self Significant Certificates (SSC) page.
The SSC device certification details are displayed.

Step 2 Select the **Enable SSC Hash Validation** check box to enable the validation of the hash key.

Step 3 Click **Apply** to commit your changes.

Configuring SSC (CLI)

Step 1 To configure hash validation of SSC, enter this command:

config certificate ssc hash validation {**enable** | **disable**}

Step 2 To see the hash key details, enter this command:
show certificate ssc

Authorizing Access Points Using MICs

You can configure controllers to use RADIUS servers to authorize access points using MICs. The controller uses an access point's MAC address as both the username and password when sending the information to a RADIUS server. For example, if the MAC address of the access point is 000b85229a70, both the username and password used by the controller to authorize the access point are 000b85229a70.

Note The lack of a strong password by the use of the access point's MAC address should not be an issue because the controller uses MIC to authenticate the access point prior to authorizing the access point through the RADIUS server. Using MIC provides strong authentication.

Note If you use the MAC address as the username and password for access point authentication on a RADIUS AAA server, do not use the same AAA server for client authentication.

Authorizing Access Points Using LSCs

You can use an LSC if you want your own public key infrastructure (PKI) to provide better security, to have control of your certificate authority (CA), and to define policies, restrictions, and usages on the generated certificates.

The LSC CA certificate is installed on access points and controllers. You need to provision the device certificate on the access point. The access point gets a signed X.509 certificate by sending a certRequest to the controller. The controller acts as a CA proxy and receives the certRequest signed by the CA for the access point.

Note When the CA server is in manual mode and if there is an AP entry in the LSC SCEP table that is pending enrollment, the controller waits for the CA server to send a pending response. If there is no response from the CA server, the controller retries a total of three times to get a response, after which the fallback mode comes into effect where the AP provisioning times out and the AP reboots and comes up with MIC.

Note LSC on controller does not take password challenge. Therefore, for LSC to work, you must disable password challenge on the CA server.

Configuring Locally Significant Certificates (GUI)

Step 1 Choose **Security** > **Certificate** > **LSC** to open the Local Significant Certificates (LSC) - General page.

Step 2 Select the **Enable LSC on Controller** check box to enable the LSC on the system.

Step 3 In the CA Server URL text box, enter the URL to the CA server. You can enter either a domain name or an IP address.

Step 4 In the Params text boxes, enter the parameters for the device certificate. The key size is a value from 384 to 2048 (in bits), and the default value is 2048.

Step 5 Click **Apply** to commit your changes.

Step 6 To add the CA certificate into the controller's CA certificate database, hover your cursor over the blue drop-down arrow for the certificate type and choose **Add**.

Step 7 Choose the **AP Provisioning** tab to open the Local Significant Certificates (LSC) - AP Provisioning page.

Step 8 Select the **Enable** check box and click **Update** to provision the LSC on the access point.

Step 9 When a message appears indicating that the access points will be rebooted, click **OK**.

Step 10 In the Number of Attempts to LSC text box, enter the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC). The range is 0 to 255 (inclusive), and the default value is 3.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Step 11 Enter the access point MAC address in the AP Ethernet MAC Addresses text box and click **Add** to add access points to the provision list.

Note To remove an access point from the provision list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning. If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 12 Click **Apply** to commit your changes.

Step 13 Click **Save Configuration** to save your changes.

Configuring Locally Significant Certificates (CLI)

Step 1 Enable LSC on the system by entering this command:
config certificate lsc {**enable** | **disable**}

Step 2 Configure the URL to the CA server by entering this command:
config certificate lsc ca-server *http://url:port/path*

where *url* can be either a domain name or IP address.

Note You can configure only one CA server. To configure a different CA server, delete the configured CA server using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

Step 3 Add the LSC CA certificate into the controller's CA certificate database by entering this command:
config certificate lsc ca-cert {**add** | **delete**}

Step 4 Configure the parameters for the device certificate by entering this command:
config certificate lsc subject-params *country state city orgn dept e-mail*

Note The common name (CN) is generated automatically on the access point using the current MIC/SSC format C*xxxx-MacAddr*, where *xxxx* is the product number.

Step 5 Configure a key size by entering this command:
config certificate lsc other-params *keysize*

The *keysize* is a value from 384 to 2048 (in bits), and the default value is 2048.

Step 6 Add access points to the provision list by entering this command:
config certificate lsc ap-provision auth-list add *AP_mac_addr*

Note To remove access points from the provision list, enter the **config certificate lsc ap-provision auth-list delete** *AP_mac_addr command.*

Note If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in *Step 8*). If you do not configure an access point provision list, all access points with a MIC or SSC certificate that join the controller are LSC provisioned.

Step 7 Configure the number of times that the access point attempts to join the controller using an LSC before the access point reverts to the default certificate (MIC or SSC) by entering this command:
config certificate lsc ap-provision revert-cert *retries*

where *retries* is a value from 0 to 255, and the default value is 3.

Note If you set the number of retries to a nonzero value and the access point fails to join the controller using an LSC after the configured number of retries, the access point reverts to the default certificate. If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate.

Note If you are configuring LSC for the first time, Cisco recommends that you configure a nonzero value.

Step 8 Provision the LSC on the access point by entering this command:
config certificate lsc ap-provision {**enable** | **disable**}

Step 9 See the LSC summary by entering this command:
show certificate lsc summary

Information similar to the following appears:

```
LSC Enabled..................................... Yes
LSC CA-Server................................... http://10.0.0.1:8080/caserver

LSC AP-Provisioning............................. Yes
 Provision-List................................. Not Configured
 LSC Revert Count in AP reboots................. 3

LSC Params:
 Country........................................ 4
```

```
 State.......................................... ca
 City........................................... ss
 Orgn........................................... org
 Dept........................................... dep
 Email.......................................... dep@co.com
 KeySize........................................ 390

LSC Certs:
 CA Cert........................................ Not Configured
 RA Cert........................................ Not Configured
```

Step 10 See details about the access points that are provisioned using LSC by entering this command:
show certificate lsc ap-provision

Information similar to the following appears:

```
LSC AP-Provisioning..... Yes
Provision-List..... Present

Idx  Mac Address
---  ------------
1  00:18:74:c7:c0:90
```

Authorizing Access Points (GUI)

Step 1 Choose **Security** > **AAA** > **AP Policies** to open the AP Policies page.

Step 2 If you want the access point to accept self-signed certificates (SSCs), manufactured-installed certificates (MICs), or local significant certificates (LSCs), select the appropriate check box.

Step 3 If you want the access points to be authorized using a AAA RADIUS server, select the **Authorize MIC APs against auth-list or AAA** check box.

Step 4 If you want the access points to be authorized using an LSC, select the **Authorize LSC APs against auth-list** check box.
Enter the Ethernet MAC address for all APs except when in bridge mode (where you need to enter the radio Mac address).

Step 5 Click **Apply** to commit your changes.

Step 6 Follow these steps to add an access point to the controller's authorization list:

a) Click **Add** to access the Add AP to Authorization List area.
b) In the MAC Address text box, enter the MAC address of the access point.
c) From the Certificate Type drop-down list, choose **MIC**, **SSC**, or **LSC**.
d) Click **Add**. The access point appears in the access point authorization list.

Note To remove an access point from the authorization list, hover your cursor over the blue drop-down arrow for the access point and choose **Remove**.

Note To search for a specific access point in the authorization list, enter the MAC address of the access point in the Search by MAC text box and click **Search**.

Authorizing Access Points (CLI)

- Configure an access point authorization policy by entering this command:
  config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **authorize-lsc-ap** {**enable** | **disable**}}
- Configure an access point to accept manufactured-installed certificates (MICs), self-signed certificates (SSCs), or local significant certificates (LSCs) by entering this command:
  config auth-list ap-policy {**mic** | **ssc** | **lsc** {**enable** | **disable**}}
- Configure the user name to be used in access point authorization requests.
  config auth-list ap-policy {**authorize-ap username** {**ap_name** | **ap_mac** | **both**}}
- Add an access point to the authorization list by entering this command:
  config auth-list add {**mic** | **ssc** | **lsc**} *ap_mac* [*ap_key*]

  where *ap_key* is an optional key hash value equal to 20 bytes or 40 digits.

Note To delete an access point from the authorization list, enter this command: **config auth-list delete ap_mac**.

- See the access point authorization list by entering this command:
  show auth-list

Configuring VLAN Tagging for CAPWAP Frames from Access Points

Information About VLAN Tagging for CAPWAP Frames from Access Points

You can configure VLAN tagging on the Ethernet interface either directly on the AP console or through the controller. The configuration is saved in the flash memory and all CAPWAP frames use the VLAN tag as configured, along with all the locally switched traffic, which is not mapped to a VLAN.

This feature is not supported on mesh access points that are in bridge mode.

Configuring VLAN Tagging for CAPWAP Frames from Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the AP name from the list of AP names to open the Details page for the AP.

Step 3 Click the **Advanced** tab.

Step 4 In the VLAN Tagging area, select the **VLAN Tagging** check box.

Step 5 In the **Trunk VLAN ID** text box, enter an ID.
If the access point is unable to route traffic through the specified trunk VLAN after about 10 minutes, the access point performs a recovery procedure by rebooting and sending CAPWAP frames in untagged mode to try and reassociate with

the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the access point is unable to route traffic through the specified trunk VLAN, it untags the packets and reassociates with the controller. The controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN.

If the trunk VLAN ID is 0, the access point untags the CAPWAP frames.

The VLAN Tag status is displayed showing whether the AP tags or untags the CAPWAP frames.

Step 6 Click **Apply**.

Step 7 You are prompted with a warning message saying that the configuration will result in a reboot of the access point. Click **OK** to continue.

Step 8 Click **Save Configuration**.

What to Do Next

After the configuration, the switch or other equipment connected to the Ethernet interface of the AP must also be configured to support tagged Ethernet frames.

Configuring VLAN Tagging for CAPWAP Frames from Access Points (CLI)

Step 1 Configure VLAN tagging for CAPWAP frames from access points by entering this command:
config ap ethernet tag {**disable** | **id** *vlan-id*} {*ap-name* | **all**}

Step 2 You can see VLAN tagging information for an AP or all APs by entering this command:
show ap ethernet tag {**summary** | *ap-name*}

Using DHCP Option 43 and DHCP Option 60

Cisco Aironet access points use the type-length-value (TLV) format for DHCP option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP option 60).

This table lists the VCI strings for Cisco access points capable of operating in lightweight mode.

Table 2: VCI Strings For Lightweight Access Points

Access Point	VCI String
Cisco Aironet 1040 Series	Cisco AP c1040
Cisco Aironet 1130 Series	Cisco AP c1130

Access Point	VCI String
Cisco Aironet 1140 Series	Cisco AP c1140
Cisco Aironet 1240 Series	Cisco AP c1240
Cisco Aironet 1250 Series	Cisco AP c1250
Cisco Aironet 1260 Series	Cisco AP c1260
Cisco Aironet 1520 Series	Cisco AP c1520
Cisco Aironet 1550 Series	Cisco AP c1550
Cisco Aironet 1700 Series	Cisco AP c1700
Cisco Aironet 2700 Series	Cisco AP c2700
Cisco Aironet 3600 Series	Cisco AP c3600
Cisco Aironet 3700 Series	Cisco AP c3700
Cisco Aironet 3500 Series	Cisco AP c3500
Cisco Aironet 700 Series	Cisco AP c700
Cisco AP801 Embedded Access Point	Cisco AP801
Cisco AP802 Embedded Access Point	Cisco AP802

The format of the TLV block is as follows:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of the IP addresses of controller management interfaces

See the product documentation for your DHCP server for instructions on configuring DHCP option 43. The *Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode* document contains example steps for configuring option 43 on a DHCP server.

If the access point is ordered with the Service Provider Option - AIR-OPT60-DHCP selected, the VCI string for that access point will be different than those listed above. The VCI string will have the “ServiceProvider”. For example, a 1260 with this option will return this VCI string: "Cisco AP c1260-ServiceProvider".

Note The controller IP address that you obtain from the DHCP server should be a unicast IP address. Do not configure the controller IP address as a multicast address when configuring DHCP Option 43.

Troubleshooting the Access Point Join Process

Access points can fail to join a controller for many reasons such as a RADIUS authorization is pending, self-signed certificates are not enabled on the controller, the access point and controller's regulatory domains do not match, and so on.

Controller software release 5.2 or later releases enable you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point, so it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining issues without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to this controller and maintains information for any access points that have successfully joined this controller.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

You can view join-related information for the following numbers of access points:

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

If any of these conditions are met and the access point has not yet joined a controller, you can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

You can also configure the syslog server IP address through the access point CLI, provided the access point is currently not connected to the controller by entering the **capwap ap log-server** *syslog_server_IP_address command.*

When the access point joins a controller for the first time, the controller pushes the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address, until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global** *syslog_server_IP_address* command. In this case, the controller pushes the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific** *Cisco_AP syslog_server_IP_address* command. In this case, the controller pushes the new specific syslog server IP address to the access point.
- The access point gets disconnected from the controller, and the syslog server IP address has been configured from the access point CLI using the **lwapp ap log-server** *syslog_server_IP_address* command. This command works only if the access point is not connected to any controller.
- The access point gets disconnected from the controller and joins another controller. In this case, the new controller pushes its global syslog server IP address to the access point.

Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address, provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points using the controller GUI and view the access point join information using the controller GUI or CLI.

Note When an AP in a Release 8.0 image tries to join Cisco WLC, Release 8.3 (having Release 8.2 as the primary image and Release 8.2.1 as the secondary image on Flash), the AP goes into a perpetual loop. (Note that the release numbers are used only as an example to illustrate the scenario of three different images and does not apply to the releases mentioned.) This loop occurs due to version mismatch. After the download, when the AP compares its image with the Cisco WLC image, there will be a version mismatch. The AP will start the entire process again, resulting in a loop.

Configuring the Syslog Server for Access Points (CLI)

Step 1 Perform one of the following:

- To configure a global syslog server for all access points that join this controller, enter this command:
  config ap syslog host global *syslog_server_IP_address*

  Note By default, the global syslog server IPv4/IPv6 address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

  Note Only one Syslog Server is used for both IPv4 and IPv6.
- To configure a syslog server for a specific access point, enter this command:
  config ap syslog host specific *Cisco_AP syslog_server_IP_address*

  Note By default, the syslog server IPv4/IPv6 address for each access point is 0.0.0.0, which indicates that the access point is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

Step 2 Enter the **save config** command to save your changes.

Step 3 See the global syslog server settings for all access points that join the controller by entering this command:
show ap config global

Information similar to the following appears:

```
AP global system logging host..................... 255.255.255.255
```

Step 4 See the syslog server settings for a specific access point by entering this command:
show ap config general *Cisco_AP*

Viewing Access Point Join Information

Join statistics for an access point that sends a CAPWAP discovery request to the controller at least once are maintained on the controller even if the access point is rebooted or disconnected. These statistics are removed only when the controller is rebooted or when you choose to clear the statistics.

Viewing Access Point Join Information (GUI)

Step 1 Choose **Monitor** > **Statistics** > **AP Join** to open the AP Join Stats page.
This page lists all of the access points that are joined to the controller or that have tried to join. It shows the radio MAC address, access point name, current join status, Ethernet MAC address, IP address, and last join time for each access point.

The total number of access points appears in the upper right-hand corner of the page. If the list of access points spans multiple pages, you can view these pages by clicking the page number links. Each page shows the join statistics for up to 25 access points.

Note If you want to remove an access point from the list, hover your cursor over the blue drop-down arrow for that access point and click **Remove**.

Note If you want to clear the statistics for all access points and start over, click **Clear Stats on All APs**.

Step 2 If you want to search for specific access points in the list of access points on the AP Join Stats page, follow these steps to create a filter to display only access points that meet certain criteria (such as MAC address or access point name).

Note This feature is especially useful if your list of access points spans multiple pages, preventing you from viewing them all at once.

a) Click **Change Filter** to open the Search AP dialog box.

b) Select one of the following check boxes to specify the criteria used when displaying access points:

- **MAC Address—**Enter the base radio MAC address of an access point.
- **AP Name—**Enter the name of an access point.

  Note When you enable one of these filters, the other filter is disabled automatically.

c) Click **Find** to commit your changes. Only the access points that match your search criteria appear on the AP Join Stats page, and the Current Filter parameter at the top of the page specifies the filter used to generate the list (for example, MAC Address:00:1e:f7:75:0a:a0 or AP Name:pmsk-ap).

Note If you want to remove the filter and display the entire access point list, click **Clear Filter**.

Step 3 To see detailed join statistics for a specific access point, click the radio MAC address of the access point. The AP Join Stats Detail page appears.
This page provides information from the controller's perspective on each phase of the join process and shows any errors that have occurred.

Viewing Access Point Join Information (CLI)

Use these CLI commands to see access point join information:

- See the MAC addresses of all the access points that are joined to the controller or that have tried to join by entering this command:

  show ap join stats summary all

- See the last join error detail for a specific access point by entering this command:

  show ap join stats summary *ap_mac*

  where *ap_mac* is the MAC address of the 802.11 radio interface.

Note To obtain the MAC address of the 802.11 radio interface, enter the **show interfaces Dot11Radio 0** command on the access point.

Information similar to the following appears:

```
Is the AP currently connected to controller..... Yes
Time at which the AP joined this controller last time...... Aug 21
12:50:36.061
Type of error that occurred last..... AP got or has
 been disconnected
Reason for error that occurred last..... The AP has
been reset by the controller
Time at which the last join error occurred..... Aug 21
12:50:34.374
```

- See all join-related statistics collected for a specific access point by entering this command:

  show ap join stats detailed *ap_mac*

  Information similar to the following appears:

```
Discovery phase statistics
- Discovery requests received..... 2
- Successful discovery responses sent..... 2
- Unsuccessful discovery request processing..... 0
- Reason for last unsuccessful discovery attempt..... Not applicable
- Time at last successful discovery attempt..... Aug 21 12:50:23.335
- Time at last unsuccessful discovery attempt..... Not applicable

Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 1
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt..... RADIUS authorization
 is pending for the AP
- Time at last successful join attempt..... Aug 21 12:50:34.481
- Time at last unsuccessful join attempt..... Aug 21 12:50:34.374

Configuration phase statistics
- Configuration requests received..... 1
- Successful configuration responses sent..... 1
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt..... Not applicable
- Time at last successful configuration attempt..... Aug 21 12:50:34.374
- Time at last unsuccessful configuration attempt..... Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure..... Not applicable
```

```
Last AP disconnect details
- Reason for last AP connection failure..... The AP has been reset by
the controller

Last join error summary
- Type of error that occurred last..... AP got or has been
disconnected
- Reason for error that occurred last..... The AP has been reset by
the controller
- Time at which the last join error occurred..... Aug 21 12:50:34.374
```

- Clear the join statistics for all access points or for a specific access point by entering this command:

  clear ap join stats {**all** | *ap_mac*}

Sending Debug Commands to Access Points Converted to Lightweight Mode

You can enable the controller to send debug commands to an access point converted to lightweight mode by entering this command:

debug ap {**enable** | **disable** | **command** *cmd*} *Cisco_AP*

When this feature is enabled, the controller sends debug commands to the converted access point as character strings. You can send any debug command supported by Cisco Aironet access points that run Cisco IOS software in lightweight mode.

Understanding How Converted Access Points Send Crash Information to the Controller

When a converted access point unexpectedly reboots, the access point stores a crash file on its local flash memory at the time of the crash. After the unit reboots, it sends the reason for the reboot to the controller. If the unit rebooted because of a crash, the controller pulls up the crash file using existing CAPWAP messages and stores it in the controller flash memory. The crash info copy is removed from the access point flash memory when the controller pulls it from the access point.

Understanding How Converted Access Points Send Radio Core Dumps to the Controller

When a radio module in a converted access point generates a core dump, the access point stores the core dump file of the radio on its local flash memory at the time of the radio crash. It sends a notification message to the controller indicating which radio generated a core dump file. The controller sends a trap that alerts you so that you can retrieve the radio core file from the access point.

The retrieved core file is stored in the controller flash and can be uploaded through TFTP or FTP to an external server for analysis. The core file is removed from the access point flash memory when the controller pulls it from the access point.

Retrieving Radio Core Dumps (CLI)

Step 1 Transfer the radio core dump file from the access point to the controller by entering this command:
config ap crash-file get-radio-core-dump *slot Cisco_AP*

For the *slot* parameter, enter the slot ID of the radio that crashed.

Step 2 Verify that the file was downloaded to the controller by entering this command:
show ap crash-file

Uploading Radio Core Dumps (GUI)

Step 1 Choose **Commands** > **Upload File** to open the Upload File from Controller page.

Step 2 From the File Type drop-down list, choose **Radio Core Dump**.

Step 3 From the Transfer Mode drop-down list, choose from the following options:

- **TFTP**
- **FTP**

Step 4 In the IP Address text box, enter the IP address of the server.

Step 5 In the File Path text box, enter the directory path of the file.

Step 6 In the File Name text box, enter the name of the radio core dump file.

Note The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

Step 7 If you chose FTP as the Transfer Mode, follow these steps:

a) In the Server Login Username text box, enter the FTP server login name.
b) In the Server Login Password text box, enter the FTP server login password.
c) In the Server Port Number text box, enter the port number of the FTP server. The default value for the server port is 21.

Step 8 Click **Upload** to upload the radio core dump file from the controller. A message appears indicating the status of the upload.

Uploading Radio Core Dumps (CLI)

Step 1 Transfer the file from the controller to a server by entering these commands:

- **transfer upload mode** {**tftp** | **ftp**}
- **transfer upload datatype radio-core-dump**
- **transfer upload serverip** *server_ip_address*
- **transfer upload path** *server_path_to_file*
- **transfer upload filename** *filename*

Note The *filename* that you enter should match the filename generated on the controller. You can determine the *filename* on the controller by entering the **show ap crash-file** command.

Note Ensure that the *filename* and *server_path_to_file* do not contain these special characters: \, :, *, ?, ", <, >, and |. You can use only / (forward slash) as the path separator. If you use the disallowed special characters in the filename, then the special characters are replaced with _ (underscores); and if you use the disallowed special characters in the *server_path_to_file*, then the path is set to the root path.

Step 2 If you are using an FTP server, also enter these commands:

- **transfer upload username** *username*
- **transfer upload password** *password*
- **transfer upload port** *port*

Note The default value for the *port* parameter is 21.

Step 3 View the updated settings by entering this command:
transfer upload start

Step 4 When prompted to confirm the current settings and start the software upload, answer **y**.

Uploading Memory Core Dumps from Converted Access Points

By default, access points converted to lightweight mode do not send memory core dumps to the controller. This section provides instructions to upload access point core dumps using the controller GUI or CLI.

Uploading Access Point Core Dumps (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** > *access point name* > and choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 2 Select the **AP Core Dump** check box to upload a core dump of the access point.

Step 3 In the TFTP Server IP text box, enter the IP address of the TFTP server.

Step 4 In the File Name text box, enter a name of the access point core dump file (such as *dump.log*).

Step 5 Select the **File Compression** check box to compress the access point core dump file. When you enable this option, the file is saved with a .gz extension (such as *dump.log.gz*). This file can be opened with WinZip.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Save Configuration** to save your changes.

Uploading Access Point Core Dumps (CLI)

Step 1 Upload a core dump of the access point by entering this command on the controller:
config ap core-dump enable *tftp_server_ip_address filename* {**compress** | **uncompress**} {*ap_name* | **all**}

where

- *tftp_server_ip_address* is the IP address of the TFTP server to which the access point sends core dump files.

  Note The access point must be able to reach the TFTP server.

- *filename* is the name that the access points uses to label the core file.
- **compress** configures the access point to send compressed core files whereas **uncompress** configures the access point to send uncompressed core files.

  Note When you choose **compress**, the file is saved with a .gz extension (for example, dump.log.gz). This file can be opened with WinZip.

- *ap_name* is the name of a specific access point for which core dumps are uploaded and **all** is all access points converted to lightweight mode.

Step 2 Enter the **save config** command to save your changes.

Viewing the AP Crash Log Information

Whenever the controller reboots or upgrades, the AP crash log information gets deleted from the controller. We recommend that you make a backup of AP crash log information before rebooting or upgrading the controller.

Viewing the AP Crash Log information (GUI)

- Choose **Management** > **Tech Support** > **AP Crash Log** to open the AP Crash Logs page.

Viewing the AP Crash Log information (CLI)

Step 1 Verify that the crash file was downloaded to the controller by entering this command:
show ap crash-file

Information similar to the following appears:

```
Local Core Files:
lrad_AP1130.rdump0 (156)
The number in parentheses indicates the size of the file. The size should be greater than zero if a
 core dump file is available.
```

Step 2 See the contents of the AP crash log file by entering this command:
show ap crash-file *Cisoc_AP*

Displaying MAC Addresses for Converted Access Points

There are some differences in the way that controllers display the MAC addresses of converted access points on information pages in the controller GUI:

- On the AP Summary page, the controller lists the Ethernet MAC addresses of converted access points.
- On the AP Detail page, the controller lists the BSS MAC addresses and Ethernet MAC addresses of converted access points.
- On the Radio Summary page, the controller lists converted access points by radio MAC address.

Disabling the Reset Button on Access Points Converted to Lightweight Mode

You can disable the reset button on access points converted to lightweight mode. The reset button is labeled MODE on the outside of the access point.

Use this command to disable or enable the reset button on one or all converted access points associated to a controller:

config ap rst-button {**enable** | **disable**} {*ap-name*}

The reset button on converted access points is enabled by default.

Configuring a Static IP Address on a Lightweight Access Point

If you want to specify an IP address for an access point rather than having one assigned automatically by a DHCP server, you can use the controller GUI or CLI to configure a static IP address for the access point. Static IP addresses are generally used only for deployments with a limited number of APs.

An access point cannot discover the controller using domain name system (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.

Note If you configure an access point to use a static IP address that is not on the same subnet on which the access point's previous DHCP address was, the access point falls back to a DHCP address after the access point reboots. If the access point falls back to a DHCP address, enter the **show ap config general** *Cisco_AP* CLI command to show that the access point is using a fallback IP address. However, the GUI shows both the static IP address and the DHCP address, but it does not identify the DHCP address as a fallback address.

Configuring a Static IP Address (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure a static IP address. The All APs > Details for (General) page appears.

Step 3 Under IP Config, select the **Static IP (IPv4/IPv6)** check box if you want to assign a static IP address to this access point. The default value is unselected.

Note The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

Step 4 Enter the static IPv4/IPv6 address of the access point, subnet mask/ prefix length assigned to the access point IPv4/IPv6 address, and the IPv4/IPv6 gateway of the access point in the corresponding text boxes.

Step 5 Click **Apply** to commit your changes. The access point reboots and rejoins the controller, and the static IPv4/IPv6 address that you specified in Step 4 is sent to the access point.

Step 6 After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNS server IP address and domain name as follows:

a) In the DNS IP Address text box, enter the IPv4/IPv6 address of the DNS server.
b) In the Domain Name text box, enter the name of the domain to which the access point belongs.
c) Click **Apply** to commit your changes.
d) Click **Save Configuration** to save your changes.

Configuring a Static IP Address (CLI)

Step 1 Configure a static IP address on the access point by entering this command:
For IPv4**—config ap static-ip enable** *Cisco_AP ip_address mask gateway*

For IPv6**—config ap static-ip enable** *Cisco_AP ip_address prefix_length gateway*

Note To disable static IP for the access point, enter the **config ap static-ip disable** *Cisco_AP* command.

Note The static IP configured on the AP will take precedence over the preferred mode configured on the AP. For example: If AP has static IPV6 address and prefer-mode is set to IPV4, then the AP will join over IPv6.

Step 2 Enter the **save config** command to save your changes.
The access point reboots and rejoins the controller, and the static IP address that you specified in Step 1 is pushed to the access point.

Step 3 After the static IPv4/IPv6 address has been sent to the access point, you can configure the DNSv4/DNSv6 server IP address and domain name as follows:

a) To specify a DNSv4/DNSv6 server so that a specific access point or all access points can discover the controller using DNS resolution, enter this command:
config ap static-ip add nameserver {*Cisco_AP* | **all**} *ip_address*

Note To delete a DNSv4/DNSv6 server for a specific access point or all access points, enter the **config ap static-ip delete nameserver** {*Cisco_AP* | **all**} command.

b) To specify the domain to which a specific access point or all access points belong, enter this command:
config ap static-ip add domain {*Cisco_AP* | **all**} *domain_name*

Note To delete a domain for a specific access point or all access points, enter this command: **config ap static-ip delete domain** {*Cisco_AP* | **all**}.

c) Enter the **save config** command to save your changes.

Step 4 See the IPv4/IPv6 address configuration for the access point by entering this command:

- For IPv4:
show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>

Cisco AP Identifier.............................. 4
Cisco AP Name.................................... AP6
...
IP Address Configuration......................... Static IP assigned
IP Address....................................... 10.10.10.118
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.10.10.1

Domain........................................... Domain1
Name Server...................................... 10.10.10.205
...
```

- For IPv6:
show ap config general *Cisco_AP*

  Information similar to the following appears:

```
show ap config general <Cisco_AP>
```

```
Cisco AP Identifier.............................. 16
Cisco AP Name.................................... AP2602I-A-K9-1
...
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:2:16:1ae:a1da:c2c7:44b
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::c60a:cbff:fe79:53c4
NAT External IP Address.......................... None

...
IPv6 Capwap UDP Lite............................. Enabled
Capwap Prefer Mode............................... Ipv6 (ApGroup Config)
Hotspot Venue Group.............................. Unspecified
Hotspot Venue Type............................... Unspecified
DNS server IP ..................... Not Available
```

Supporting Oversized Access Point Images

Controller software release 5.0 or later releases allow you to upgrade to an oversized access point image by automatically deleting the recovery image to create sufficient space.

The recovery image provides a backup image that can be used if an access point power-cycles during an image upgrade. The best way to avoid the need for access point recovery is to prevent an access point from power-cycling during a system upgrade. If a power-cycle occurs during an upgrade to an oversized access point image, you can recover the access point using the TFTP recovery procedure.

Recovering the Access Point—Using the TFTP Recovery Procedure

Step 1 Download the required recovery image from Cisco.com (for example, ap3g2-rcvk9w8-tar.152-4.JB6.tar for 2700 or 3700 APs) and install it in the root directory of your TFTP server.

Step 2 Connect the TFTP server to the same subnet as the target access point and power-cycle the access point. The access point boots from the TFTP image and then joins the controller to download the oversized access point image and complete the upgrade procedure.

Step 3 After the access point has been recovered, you may remove the TFTP server.

Configuring Packet Capture

Information About Packet Capture

To resolve issues such as voice and security on wireless networks, you might need to dump packets from the AP for analysis while the AP continues to operate normally. The packets can be dumped on to an FTP server. This process of dumping packets for analysis is called Packet Capture. Use the controller to start or stop packet

capture for clients. You can choose the type of packets that need to be captured using the controller CLI from the following types:

- Management Packets
- Control Packets
- Data Packets
    - Dot1X
    - ARP
    - IAPP
    - All IP
    - UDP with matching port number
    - DHCP
    - TCP with matching port number
    - Multicast frames
    - Broadcast frames

The packets are captured and dumped in the order of arrival or transmit of packets except for beacons and probe responses. The packet capture contains information such as channel, RSSI, data rate, SNR, and timestamp. Each packet is appended with additional information from the AP. You can choose to dump either just packet headers or full packets.

The following are some guidelines for packet capture:

- If FTP transfer time is slower than the packet rate, some of the packets do not appear in the capture file.
- If the buffer does not contain any packets, a known dummy packet is dumped to keep the connection alive.
- A file is created on the FTP server for each AP based on unique AP and controller name and timestamp. Ensure that the FTP server is reachable by the AP.
- If the FTP transfer fails or FTP connection is lost during packet capture, the AP stops capturing packets, notifies with an error message and SNMP trap, and a new FTP connection is established.

Restrictions for Packet Capture

- Packet capture can be enabled for only one client.
- This feature is not supported in intercontroller roaming scenarios. If you know the AP or the controller to which the client is going to roam, you can configure the packet capture for the client in the new controller or AP using the CLI.
- Not all packets in the air are captured, but only those that reach the radio driver.
- By default, a packet capture process is stopped after 10 minutes. You can, however, configure the packet capture to stop at any time between 1 to 60 minutes.

Configuring Packet Capture (CLI)

Step 1 Configure FTP parameters for packet capture by entering this command:
config ap packet-dump ftp serverip *ip-address* **path** *path* **username** *user_ID* **password** *password*

Step 2 Start or stop packet capture by entering this command:
config ap packet-dump {**start** *client-mac-address ap-name* | **stop**}

Step 3 Configure the buffer size for packet capture by entering this command:
config ap packet-dump buffer-size *size-in-kb*

Step 4 Configure the time for packet capture by entering this command:
config ap packet-dump capture-time *time-in-minutes*

The valid range is between 1 to 60 minutes.

Step 5 Configure the types of packets to be captured by entering this command:
config ap packet-dump classifier {**arp** | **broadcast** | **control** | **data** | **dot1x** | **iapp** | **ip** | **management** | **multicast** | {**tcp port** *port-number*} | {**udp port** *port-number*}} {**enable** | **disable**}

Step 6 Configure the packet length after truncation by entering this command:
config ap packet-dump truncate *length-in-bytes*

Step 7 Know the status of packet capture by entering this command:
show ap packet-dump status

Step 8 Configure debugging of packet capture by entering this command:
debug ap packet-dump {**enable** | **disable**}

Configuring OfficeExtend Access Points

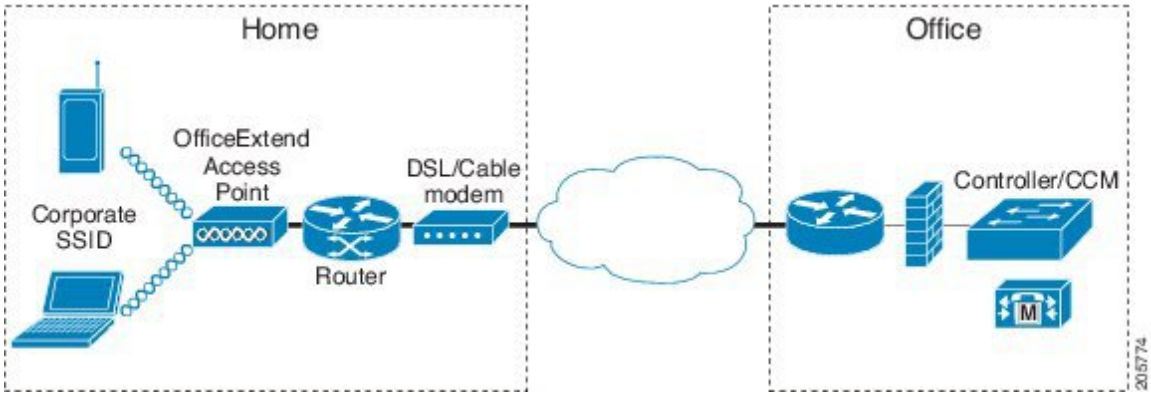
Information About OfficeExtend Access Points

A Cisco 600 Series OfficeExtend access point (Cisco OEAP) provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Note DTLS is permanently enabled on the Cisco OEAP. You cannot disable DTLS on this access point.

The following figure shows a typical OfficeExtend access point setup.

Figure 2: Typical OfficeExtend Access Point Setup



Note Cisco OEAPs are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), enabling an entire group of computers to be represented by a single IP address. There is no limit to the number of Cisco OEAPs that you can deploy behind a NAT device. Roaming is not supported for the Cisco 600 OEAP model.

All the supported indoor AP models with integrated antenna can be configured as OEAP except the AP-700I and AP-700W series access points.

OEAP 600 Series Access Points

This section details the requirements for configuring a Cisco wireless LAN controller for use with the Cisco 600 Series OfficeExtend Access Point. The 600 Series OfficeExtend Access Point supports split mode operation, and it requires configuration through the WLAN controller in local mode. This section describes the configurations necessary for proper connection and supported feature sets.

Note IPv6 is not supported on Cisco 600 Series OfficeExtend Access Points.

Note The CAPWAP UDP 5246 and 5247 ports must be open on the firewall between the WLAN controller and the 600 Series OfficeExtend Access Point.

Note Multicast is not supported on Cisco 600 Series OfficeExtend Access Points.

OEAP in Local Mode

The 600 Series OfficeExtend Access Point connects to the controller in local mode. You cannot alter these settings.

Note Monitor mode, flexconnect mode, sniffer mode, rogue detector, bridge, and SE-Connect are not supported on the 600 Series OfficeExtend Access Point and are not configurable.

Figure 3: OEAP Mode

Supported WLAN Settings for 600 Series OfficeExtend Access Point

The 600 Series OfficeExtend Access Point supports a maximum of three WLANs and one remote LAN. If your network deployment has more than three WLANs, you must place the 600 Series OfficeExtend Access Point in an AP group. If the 600 Series OfficeExtend Access Points are added to an AP group, the same limit of three WLANs and one remote LAN still applies for the configuration of the AP group.

If the 600 Series OfficeExtend Access Point is in the default group, which means that it is not in a defined AP group, the WLAN/remote LAN IDs must be set lower than ID 8.

If additional WLANs or remote LANs are created with the intent of changing the WLANs or remote LAN being used by the 600 Series OfficeExtend Access Point, you must disable the current WLANs or remote LAN that you are removing before enabling the new WLANs or remote LAN on the 600 Series OfficeExtend Access Point. If there are more than one remote LANs enabled for an AP group, disable all remote LANs and then enable only one of them.

If more than three WLANs are enabled for an AP group, disable all WLANs and then enable only three of them.

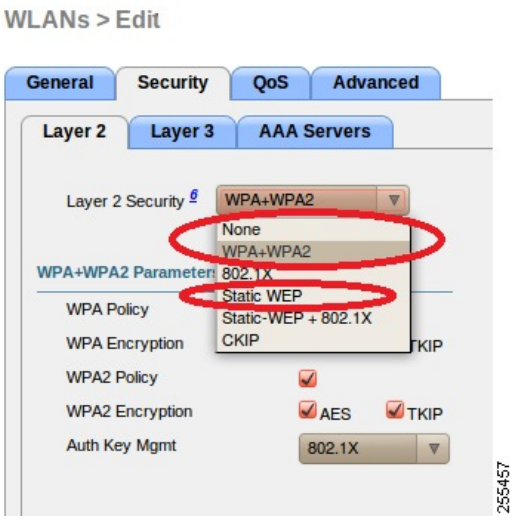
WLAN Security Settings for the 600 Series OfficeExtend Access Point

When configuring the security settings in the WLAN (see the following figure), note that there are specific elements that are not supported on the 600 Series OfficeExtend Access Point. CCX is not supported on the 600 Series OfficeExtend Access Point, and elements related to CCX are not supported.

For Layer 2 Security, the following options are supported for the 600 Series OfficeExtend Access Point:

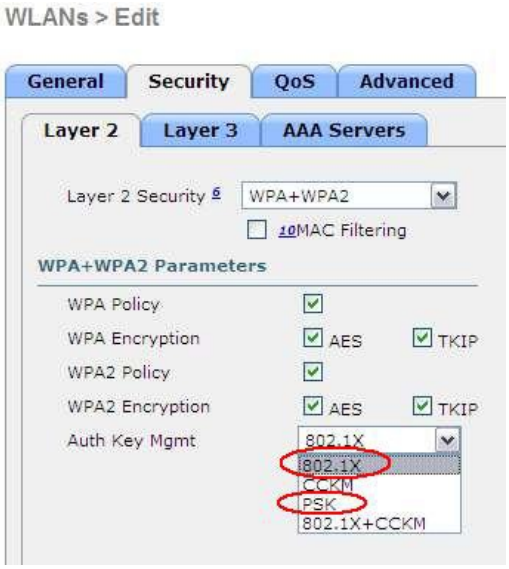
- None
- WPA+WPA2
- Static WEP
- 802.1X (only for remote LANs)

Figure 4: WLAN Layer 2 Security Settings



In the Security tab (see the following figure), do not select CCKM in WPA+WPA2 settings. Select only 802.1X or PSK.

Figure 5: WLAN Security Settings - Auth Key Management



Security encryption settings must be identical for WPA and WPA2 for TKIP and AES. The following are examples of incompatible settings for TKIP and AES.

Figure 6: Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series

Figure 7: Incompatible WPA and WPA2 Security Encryption Settings for OEAP 600 Series

The following are examples of compatible settings:

Figure 8: Compatible Security Settings for OEAP Series

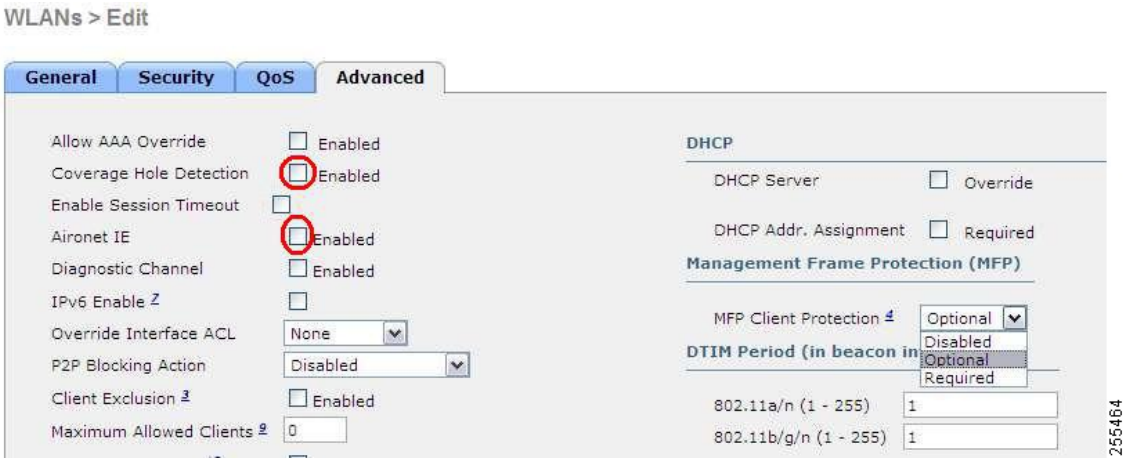
Figure 9: Compatible Security Settings for OEAP Series

QoS settings are supported (see the following figure), but CAC is not supported and should not be enabled.

Note Do not enable Coverage Hole Detection.

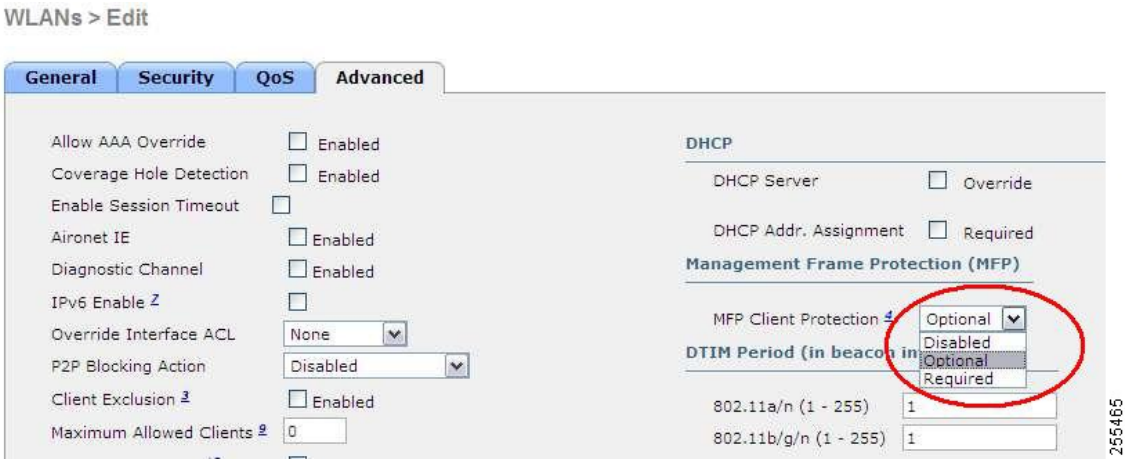
Note Aironet IE should not be enabled. This option is not supported.

Figure 10: QoS Settings for OEAP 600



MFP is also not supported and should be disabled or set to optional.

Figure 11: MFP Settings for OEAP Series Access Points



Client Load Balancing and Client Band Select are not supported.

Authentication Settings

For authentication on the 600 Series OfficeExtend Access Point, LEAP is not supported. This configuration must be addressed on the clients and RADIUS servers to migrate them to EAP-Fast, EAP-TTLS, EAP-TLS, or PEAP.

If Local EAP is being utilized on the controller, the settings would also have to be modified not to use LEAP.

Supported User Count on 600 Series OfficeExtend Access Point

Only 15 users are allowed to connect on the WLANs provided on the Cisco 600 Series OEAP at any one time, a sixteenth user cannot authenticate until one of the first clients is deauthenticated or timeout on the controller occurs. This number is cumulative across the controller WLANs on the 600 Series OfficeExtend Access Point.

For example, if two controller WLANs are configured and there are 15 users on one of the WLANs, no other users can join the other WLAN on the 600 Series OfficeExtend Access Point at that time.

This limit does not apply to the local private WLANs that the end user configures on the 600 Series OfficeExtend Access Point for personal use. Clients connected on these private WLANs or on the wired ports do not affect these limits.

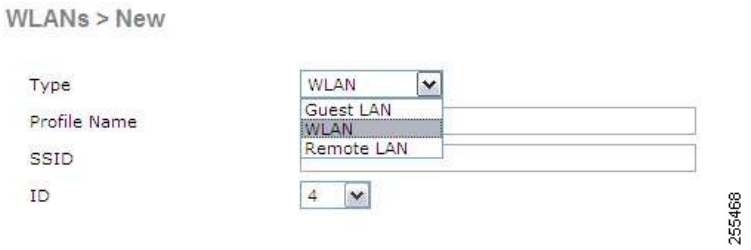
Note This limit does not apply to other AP models that operate in the OfficeExtend mode.

Remote LAN Settings

Only four clients can connect through a remote LAN port on the 600 Series OfficeExtend Access Point. This number does not affect the fifteen user limit imposed for the Controller WLANs. The remote LAN client limit supports connecting a switch or hub to the remote LAN port for multiple devices or connecting directly to a Cisco IP phone that is connected to that port. Only the first four devices can connect until one of the devices is idle for more than one minute.

Remote LAN is configured in the same way that a WLAN or Guest LAN is configured on the controller:

Figure 12: Remote LAN Settings for OEAP 600 Series AP



Security settings can be left open, set for MAC filtering, or set for Web Authentication. The default is to use MAC filtering. Additionally, you can specify 802.1X Layer 2 security settings.

Figure 13: Layer 2 Security Settings for OEAP 600 Series APs in Remote LANs

Figure 14: Layer 3 Security Settings for OEAP 600 Series APs in Remote LANs

Channel Management and Settings

The radios for the 600 Series OfficeExtend Access Point are controlled through the Local GUI on the access point and not through the Wireless LAN Controller. The Tx power and channel settings can be set manually through the controller interface. RRM is not supported on the 600 Series OfficeExtend Access Point.

The 600 series scans and chooses channels for 2.4-GHz and 5-GHz during startup as long as the default settings on the local GUI are left as default in both spectrums.

Figure 15: Channel Selection for OEAP 600 Series APs

The channel bandwidth for 5.0 GHz is also configured on the 600 Series OfficeExtend Access Point Local GUI, for 20-MHz or 40-MHz wide channels. Setting the channel width to 40 MHz for 2.4 GHz is not supported and fixed at 20 MHz.

Figure 16: Channel Width for OEAP 600 APs

Additional Caveats

- The Cisco 600 Series OfficeExtend Access Points (OEAPs) are designed for single AP deployments, therefore client roaming between Cisco 600 Series OEAPs is not supported.

  Disabling the 802.11a/n or 802.11b/g/n on the controller may not disable these spectrums on the Cisco 600 Series OEAP because local SSID may be still working.

- Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- Cisco Aironet APs other than 600 Series OEAPs that are converted to OEAP mode and mapped to locally switched WLAN forward the DHCP request to the local subnet on the AP connected switch. To avoid this condition, you must disable local switching and local authentication.
- For Cisco 600 Series OEAP to associate with Cisco Virtual Wireless LAN Controller, follow these steps:

  1. Configure the OEAP to associate with a physical controller that is using 7.5 or a later release and download the corresponding AP image.
  2. Configure the OEAP so that the OEAP does not associate with the physical controller again; for example, you can implement an ACL in the network to block CAPWAP between the OEAP and the physical controller.
  3. Configure the OEAP to associate with the Cisco Virtual Wireless LAN Controller.

Implementing Security

Note Configuring LSC is not a requirement but is an option. The OfficeExtend 600 access points do not support LSC.

1. Use local significant certificates (LSCs) to authorize your OfficeExtend access points, by following the instructions in Authorizing Access Points Using LSCs.
2. Implement AAA server validation using the access point's MAC address, name, or both as the username in authorization requests, by entering this command:

   config auth-list ap-policy authorize-ap username {*ap_mac* | *Cisco_AP* | **both**}

   Using the access point name for validation can ensure that only the OfficeExtend access points of valid employees can associate with the controller. To implement this security policy, ensure that you name each OfficeExtend access point with an employee ID or employee number. When an employee is terminated, run a script to remove this user from the AAA server database, which prevents that employee's OfficeExtend access point from joining the network.
3. Save your changes by entering this command:

   save config

Note CCX is not supported on the 600 OEAP. Elements related to CCX are not supported. Also, only 802.1X or PSK is supported. TKIP and AES security encryption settings must be identical for WPA and WPA2.

Licensing for an OfficeExtend Access Point

To use OfficeExtend access points, a base license must be installed and in use on the controller. After the license is installed, you can enable the OfficeExtend mode on the supported Cisco Aironet AP models that support OfficeExtend mode.

Configuring OfficeExtend Access Points

After Cisco Aironet access point has associated with the controller, you can configure it as an OfficeExtend access point.

Configuring OfficeExtend Access Points (GUI)

Step 1 Choose **Wireless** to open the **All APs** page.

Step 2 Click the name of the desired access point to open the **All APs > Details** page.

Step 3 Enable FlexConnect on the access point as follows:

a) In the **General** tab, choose **FlexConnect** from the **AP Mode** drop-down list to enable FlexConnect for this access point.

Step 4 Configure one or more controllers for the access point as follows:

a) Click the **High Availability** tab.

b) Enter the name and IP address of the primary controller for this access point in the **Primary Controller Name** and **Management IP Address** text boxes.

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

c) If desired, enter the name and IP address of a secondary or tertiary controller (or both) in the corresponding **Controller Name** and **Management IP Address** text boxes.

d) Click **Apply**. The access point reboots and then rejoins the controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

Step 5 Enable OfficeExtend access point settings as follows:

a) Click the **FlexConnect** tab.

b) Select the **Enable OfficeExtend AP** check box to enable the OfficeExtend mode for this access point. The default value is selected.
Unselecting this check box disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter **clear ap config** *Cisco_AP* on the controller CLI. If you want to clear only the access point's personal SSID, click **Reset Personal SSID**.

Note The OfficeExtend AP support is enabled for all the supported Cisco Aironet integrated antenna access points.

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point by selecting the **Rogue Detection** check box on the **All APs > Details for (Advanced)** page. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point by selecting the **Data Encryption** check box on the **All APs > Details for (Advanced)** page.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by selecting the **Telnet** or **SSH** check box on the **All APs > Details for (Advanced)** page.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point by selecting the **Enable Link Latency** check box on the All APs > Details for (Advanced) page.

c) Select the **Enable Least Latency Controller Join** check box if you want the access point to choose the controller with the least latency when joining. Otherwise, leave this check box unselected, which is the default value. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.

d) Click **Apply**.
The **OfficeExtend AP** text box on the All APs page shows which access points are configured as OfficeExtend access points.

Step 6 Configure a specific username and password for the OfficeExtend access point so that the user at home can log into the GUI of the OfficeExtend access point:

a) Click the **Credentials** tab.

b) Select the **Over-ride Global Credentials** check box to prevent this access point from inheriting the global username, password, and enable password from the controller. The default value is unselected.

c) In the **Username**, **Password**, and **Enable Password** text boxes, enter the unique username, password, and enable password that you want to assign to this access point.

Note The information that you enter is retained across controller and access point reboots and if the access point joins a new controller.

d) Click **Apply**.

Note If you want to force this access point to use the controller's global credentials, unselect the **Over-ride Global Credentials** check box.

Step 7 Configure access to local GUI, LAN ports, and local SSID of the OfficeExtend access points:

a) Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

b) Under OEAP Config Parameters, select or unselect the **Disable Local Access** check box to enable or disable local access of the OfficeExtend access points.

Note By default, the **Disable Local Access** check box is unselected and therefore the Ethernet ports and personal SSIDs are enabled. This configuration does not affect remote LAN. The port is enabled only when you configure a remote LAN.

Step 8 Click **Save Configuration**.

Step 9 If your controller supports only OfficeExtend access points, see the Configuring RRM section for instructions on setting the recommended values for the DCA interval, channel scan duration, and neighbor packet frequency.

Configuring OfficeExtend Access Points (CLI)

- Enable FlexConnect on the access point by entering this command:
  config ap mode flexconnect *Cisco_AP*
- Configure one or more controllers for the access point by entering one or all of these commands:
  config ap primary-base *controller_name Cisco_AP controller_ip_address*

  config ap secondary-base *controller_name Cisco_AP controller_ip_address*

  config ap tertiary-base *controller_name Cisco_AP controller_ip_address*

Note You must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Note The names and IP addresses must be unique for the primary, secondary, and tertiary controllers.

- Enable the OfficeExtend mode for this access point by entering this command:
  config flexconnect office-extend {**enable** | **disable**} *Cisco_AP*

  The default value is enabled. The **disable** parameter disables OfficeExtend mode for this access point. It does not undo all of the configuration settings on the access point. If you want to clear the access point's configuration and return it to the factory-default settings, enter this command:

  clear ap config *cisco-ap*

  If you want to clear only the access point's personal SSID, enter this command:

  config flexconnect office-extend clear-personalssid-config *Cisco_AP.*

Note Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable rogue detection for a specific access point or for all access points using the **config rogue detection** {**enable** | **disable**} {*Cisco_AP* | **all**} command. Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices.

Note DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points using the **config ap link-encryption** {**enable** | **disable**} {*Cisco_AP* | **all**} command.

Note Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point using the **config ap** {**telnet** | **ssh**} {**enable** | **disable**} *Cisco_AP* command.

Note Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller using the **config ap link-latency** {**enable** | **disable**} {*Cisco_AP* | **all**} command.

- Enable the access point to choose the controller with the least latency when joining by entering this command:
  config flexconnect join min-latency {**enable** | **disable**} *Cisco_AP*

  The default value is disabled. When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the Cisco 5500 Series Controller that responds first.
- Configure a specific username and password that users at home can enter to log into the GUI of the OfficeExtend access point by entering this command:
  config ap mgmtuser add username *user* **password** *password* **enablesecret** *enable_password Cisco_AP*

  The credentials that you enter in this command are retained across controller and access point reboots and if the access point joins a new controller.

Note If you want to force this access point to use the controller's global credentials, enter the **config ap mgmtuser delete** *Cisco_AP* command. The following message appears after you execute this command: "AP reverted to global username configuration."

- To configure access to the local network for the Cisco 600 Series OfficeExtend access points, enter the following command:
  config network oeap-600 local-network {**enable** | **disable**}

When disabled, the local SSIDs, local ports are inoperative; and the console is not accessible. When reset, the default restores local access. This configuration does not affect the remote LAN configuration if configured on the access points.

- Configure the Dual R-LAN Ports feature, which allows the Ethernet port 3 of Cisco 600 Series OfficeExtend access points to operate as a remote LAN by entering this command:
  config network oeap-600 dual-rlan-ports {**enable** | **disable**}

  This configuration is global to the controller and is stored by the AP and the NVRAM variable. When this variable is set, the behavior of the remote LAN is changed. This feature supports different remote LANs per remote LAN port.

  The remote LAN mapping is different depending on whether the default group or AP Groups is used:

  - Default Group—If you are using the default group, a single remote LAN with an even numbered remote LAN ID is mapped to port 4. For example, a remote LAN with remote LAN ID 2 is mapped to port 4 (on the Cisco 600 OEAP). The remote LAN with an odd numbered remote LAN ID is mapped to port 3 (on the Cisco 600 OEAP). For example, a remote LAN with remote LAN ID 1 is mapped to port 3 (on the Cisco 600 OEAP).
  - AP Groups—If you are using an AP group, the mapping to the OEAP-600 ports is determined by the order of the AP groups. To use an AP group, you must first delete all remote LANs and WLANs from the AP group leaving it empty. Then, add the two remote LANs to the AP group adding the port 3 AP remote LAN first, and the port 4 remote group second, followed by any WLANs.

- Save your changes by entering this command:
  save config

Note If your controller supports only OfficeExtend access points, see the Configuring Radio Resource Management section for instructions on setting the recommended value for the DCA interval.

Configuring a Personal SSID on an OfficeExtend Access Point Other than 600 Series OEAP

Step 1 Find the IP address of your OfficeExtend access point by doing one of the following:

- Log on to your home router and look for the IP address of your OfficeExtend access point.
- Ask your company's IT professional for the IP address of your OfficeExtend access point.
- Use an application such as Network Magic to detect devices on your network and their IP addresses.

Step 2 With the OfficeExtend access point connected to your home router, enter the IP address of the OfficeExtend access point in the Address text box of your Internet browser and click **Go**.

Note Make sure that you are not connected to your company's network using a virtual private network (VPN) connection.

Step 3 When prompted, enter the username and password to log into the access point.

Step 4 On the OfficeExtend Access Point Welcome page, click **Enter**. The OfficeExtend Access Point Home page appears.

Step 5 Choose **Configuration** to open the Configuration page.

Step 6 In the SSID text box, enter the personal SSID that you want to assign to this access point. This SSID is locally switched.

Note A controller with an OfficeExtend access point publishes only up to 15 WLANs to each connected access point because it reserves one WLAN for the personal SSID.

Step 7 From the Security drop-down list, choose **Open**, **WPA2/PSK (AES)**, or **104 bit WEP** to set the security type to be used by this access point.

Note If you choose WPA2/PSK (AES), make sure that the client is configured for WPA2/PSK and AES encryption.

Step 8 If you chose WPA2/PSK (AES) in *Step 8*, enter an 8- to 38-character WPA2 passphrase in the Secret text box. If you chose 104 bit WEP, enter a 13-character ASCII key in the Key text box.

Step 9 Click **Apply**.

Note If you want to use the OfficeExtend access point for another application, you can clear this configuration and return the access point to the factory-default settings by clicking **Clear Config**. You can also clear the access point's configuration from the controller CLI by entering the **clear ap config** *Cisco_AP* command.

These steps can be used for configuring a personal SSID on OfficeExtend access points only. See the *Aironet 600 Series OfficeExtend Access Point Configuration Guide* for information on configuring a personal SSID on OEAP 600 APs.

Viewing OfficeExtend Access Point Statistics

Use these commands to view information about the OfficeExtend access points on your network:

- See a list of all OfficeExtend access points by entering this command:

  show flexconnect office-extend summary

- See the link delay for OfficeExtend access points by entering this command:

  show flexconnect office-extend latency

- See the encryption state of all access points or a specific access point by entering this command:

  show ap link-encryption {**all** | *Cisco_AP*}

  This command also shows authentication errors, which track the number of integrity check failures, and replay errors, which track the number of times that the access point receives the same packet. See the data plane status for all access points or a specific access point by entering this command:

  show ap data-plane {**all** | *Cisco_AP*}

Using Cisco Workgroup Bridges

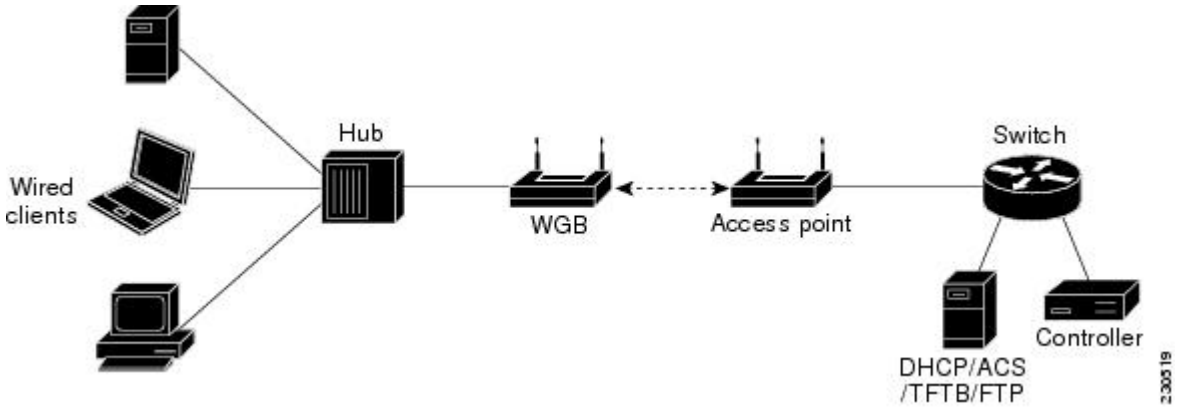
Information About Cisco Workgroup Bridges

A workgroup bridge (WGB) is a mode that can be configured on an autonomous IOS access point to provide wireless connectivity to a lightweight access point on behalf of clients that are connected by Ethernet to the

WGB access point. A WGB connects a wired network over a single wireless segment by learning the MAC addresses of its wired clients on the Ethernet interface and reporting them to the lightweight access point using Internet Access Point Protocol (IAPP) messaging. The WGB provides wireless access connectivity to wired clients by establishing a single wireless connection to the lightweight access point. The lightweight access point treats the WGB as a wireless client.

A Cisco IOS AP as a WGB using the Cisco IOS 15.2 or later releases support Protected Extensible Authentication Protocol (PEAP) with the controller.

Figure 17: WGB Example



Note If the lightweight access point fails, the WGB attempts to associate to another access point.

The following are some guidelines for Cisco Workgroup Bridges:

- The WGB can be any autonomous access point that supports the workgroup bridge mode and is running Cisco IOS Release 12.4(3g)JA or later releases (on 32-MB access points) or Cisco IOS Release 12.3(8)JEB or later releases (on 16-MB access points). These access points include the AP1120, AP1121, AP1130, AP1231, AP1240, and AP1310. Cisco IOS releases prior to 12.4(3g)JA and 12.3(8)JEB are not supported.

  Note If your access point has two radios, you can configure only one for workgroup bridge mode. This radio is used to connect to the lightweight access point. We recommend that you disable the second radio.

  Enable the workgroup bridge mode on the WGB as follows:

  - On the WGB access point GUI, choose **Workgroup Bridge** for the role in radio network on the Settings > Network Interfaces page.
  - On the WGB access point CLI, enter the **station-role workgroup-bridge command.**

Note See the sample WGB access point configuration in the WGB Configuration Example section.

- The following features are supported for use with a WGB:
  - Guest N+1 redundancy
  - Local EAP
  - Open, WEP 40, WEP 128, CKIP, WPA+TKIP, WPA2+AES, LEAP, EAP-FAST, and EAP-TLS authentication modes
- Wired clients connected to the WGB are not authenticated for security. Instead, the WGB is authenticated against the access point to which it associates. Therefore, we recommend that you physically secure the wired side of the WGB.
- Wired clients connected to a WGB inherit the WGB's QoS and AAA override attributes.
- To enable the WGB to communicate with the lightweight access point, create a WLAN and make sure that Aironet IE is enabled.
- If you have to apply ACL to WGB during run time, do not modify the ACL configuration for interface in the controller during run time. If you need to modify any ACLs, then you must disable all WLANs that are in the controller or disable both the 802.11a and 80.11b networks. Also, ensure that there are no clients associated and mapped to that interface and then you can modify the ACL settings.

Restrictions for Cisco Workgroup Bridges

- The WGB can associate only with lightweight access points.
- Only WGBs in client mode (which is the default value) are supported. Those WGBs in infrastructure mode are not supported. Perform one of the following to enable client mode on the WGB:
  - On the WGB access point GUI, choose **Disabled** for the Reliable Multicast to WGB parameter.
  - On the WGB access point CLI, enter the **no infrastructure client** command.

Note VLANs are not supported for use with WGBs.

Note See the sample WGB access point configuration in the WGB Configuration Example section.

- The following features are not supported for use with a WGB:
  - Idle timeout
  - Web authentication

Note If a WGB associates to a web-authentication WLAN, the WGB is added to the exclusion list, and all of the WGB wired clients are deleted.

- The WGB supports a maximum of 20 wired clients. If you have more than 20 wired clients, use a bridge or another device.
- The DirectStream feature from the controller does not work for clients behind workgroup bridges and the stream is denied.
- With Layer 3 roaming, if you plug a wired client into the WGB network after the WGB has roamed to another controller (for example, to a foreign controller), the wired client's IP address displays only on the anchor controller, not on the foreign controller.
- If a wired client does not send traffic for an extended period of time, the WGB removes the client from its bridge table, even if traffic is continuously being sent to the wired client. As a result, the traffic flow to the wired client fails. To avoid the traffic loss, prevent the wired client from being removed from the bridge table by configuring the aging-out timer on the WGB to a large value using the following Cisco IOS commands on the WGB:

  ```
  configure terminal
  bridge bridge-group-number aging-time seconds
  exit
  end
  ```

  where *bridge-group-number* is a value between 1 and 255, and *seconds* is a value between 10 and 1,000,000 seconds. We recommend configuring the *seconds* parameter to a value greater than the wired client's idle period.
- When you delete a WGB record from the controller, all of the WGB wired clients' records are also deleted.
- These features are not supported for wired clients connected to a WGB:
  - MAC filtering
  - Link tests
  - Idle timeout
- The broadcast forwarding toward wired WGB clients works only on the native VLAN. If additional VLANs are configured, only the native VLAN forwards broadcast traffic.
- Wired clients behind a WGB cannot connect to a DMZ/Anchor controller. To enable wired clients behind a WGB to connect to an anchor controller in a DMZ, you must enable VLANs in the WGB using the **config wgb vlan enable** command.
- The **dot11 arp-cache** global configuration command that you can enter on the access point that is in WGB mode is not supported.
- WGB clients do not show enc-cipher and AKM because they are wired clients. WGB APs, however, show correct values of enc-cipher and AKM.

WGB Configuration Example

The following is an example of the configuration of a WGB access point using static WEP with a 40-bit WEP key:

```
ap# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ap(config)# dot11 ssid WGB_with_static_WEP
ap(config-ssid)# authentication open
ap(config-ssid)# guest-mode
ap(config-ssid)# exit
ap(config)# interface  dot11Radio 0
ap(config)# station-role workgroup-bridge
ap(config-if)# encry mode wep 40
ap(config-if)# encry key 1 size 40 0 1234567890
ap(config-if)# ssid WGB_with_static_WEP
ap(config-if)# end
```

Verify that the WGB is associated to an access point by entering this command on the WGB:

show dot11 association

Information similar to the following appears:

```
ap# show dot11 associations
802.11 Client Stations on Dot11Radio0:
SSID [FCVTESTING] :
MAC Address    IP address      Device        Name            Parent         State
000b.8581.6aee 10.11.12.1      WGB-client    map1            -              Assoc
ap#
```

Viewing the Status of Workgroup Bridges (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.
The WGB text box on the right side of the page indicates whether any of the clients on your network are workgroup bridges.

Step 2 Click the MAC address of the desired client. The Clients > Detail page appears.
The Client Type text box under Client Properties shows “WGB” if this client is a workgroup bridge, and the Number of Wired Client(s) text box shows the number of wired clients that are connected to this WGB.

Step 3 See the details of any wired clients that are connected to a particular WGB as follows:

a) Click **Back** on the Clients > Detail page to return to the Clients page.

b) Hover your cursor over the blue drop-down arrow for the desired WGB and choose **Show Wired Clients**. The WGB Wired Clients page appears.

Note If you want to disable or remove a particular client, hover your cursor over the blue drop-down arrow for the desired client and choose **Remove** or **Disable**, respectively.

c) Click the MAC address of the desired client to see more details for this particular client. The Clients > Detail page appears.

The Client Type text box under Client Properties shows “WGB Client,” and the rest of the text boxes on this page provide additional information for this client.

Viewing the Status of Workgroup Bridges (CLI)

Step 1 See any WGBs on your network by entering this command:
show wgb summary

Step 2 See the details of any wired clients that are connected to a particular WGB by entering this command:
show wgb detail *wgb_mac_address*

Debugging WGB Issues (CLI)

Before You Begin

- Enable debugging for IAPP messages, errors, and packets by entering these commands:
  - **debug iapp all enable—**Enables debugging for IAPP messages.
  - **debug iapp error enable—**Enables debugging for IAPP error events.
  - **debug iapp packet enable—**Enables debugging for IAPP packets.
- Debug an roaming issue by entering this command:
  debug mobility handoff enable
- Debug an IP assignment issue when DHCP is used by entering these commands:
  - **debug dhcp message enable**
  - **debug dhcp packet enable**
- Debug an IP assignment issue when static IP is used by entering these commands:
  - **debug dot11 mobile enable**
  - **debug dot11 state enable**

Using Non-Cisco Workgroup Bridges

Information About Non-Cisco Workgroup Bridges

When a Cisco workgroup bridge (WGB) is used, the WGB informs the access points of all the clients that it is associated with. The controller is aware of the clients associated with the access point. When non-Cisco WGBs are used, the controller has no information about the IP address of the clients on the wired segment behind the WGB. Without this information, the controller drops the following types of messages:

- ARP REQ from the distribution system for the WGB client
- ARP RPLY from the WGB client
- DHCP REQ from the WGB client
- DHCP RPLY for the WGB client

The following are some guidelines for non-Cisco workgroup bridges:

- The controller can accommodate non-Cisco WGBs so that the controller can forward ARP, DHCP, and data traffic to and from the wired clients behind workgroup bridges by enabling the passive client feature. To configure your controller to work with non-Cisco WGBs, you must enable the passive client feature so that all traffic from the wired clients is routed through the WGB to the access point. All traffic from the wired clients is routed through the work group bridge to the access point.

  Note For FlexConnect APs in local switching, non-Cisco workgroup-bridge clients in bridged mode are supported using the **config flexconnect group** *group-name* **dhcp overridden-interface enable** command.

- When a WGB wired client leaves a multicast group, the downstream multicast traffic to other WGB wired clients is interrupted briefly.
- If you have clients that use PC virtualization software such as VMware, you must enable this feature.

  Note We have tested multiple third-party devices for compatibility but cannot ensure that all non-Cisco devices work. Support for any interaction or configuration details on the third-party device should be discussed with the device manufacturer.

- You must enable the passive client functionality for all non-Cisco workgroup bridges.
- You might need to use the following commands to configure DHCP on clients:
  - Disable DHCP proxy by using the **config dhcp proxy disable** command.
  - Enable DHCP boot broadcast by using the **config dhcp proxy disable bootp-broadcast enable** command.

Restrictions for Non-Cisco Workgroup Bridges

- Only Layer 2 roaming is supported for WGB devices.
- Layer 3 security (web authentication) is not support for WGB clients.
- Visibility of wired hosts behind a WGB on a controller is not supported because the non-Cisco WGB device performs MAC hiding. Cisco WGB supports IAPP.
- ARP poisoning detection does not work on a WLAN when the flag is enabled.
- VLAN select is not supported for WGB clients.
- Some third-party WGBs need to operate in non-DHCP relay mode. If problems occur with the DHCP assignment on devices behind the non-Cisco WGB, use the **config dhcp proxy disable** and **config dhcp proxy disable bootp-broadcast disable** commands.

  The default state is DHCP proxy enabled. The best combination depends on the third-party characteristics and configuration.

Configuring Backup Controllers

Information About Configuring Backup Controllers

A single controller at a centralized location can act as a backup for access points when they lose connectivity with the primary controller in the local region. Centralized and regional controllers do not need to be in the same mobility group. You can specify a primary, secondary, and tertiary controller for specific access points in your network. Using the controller GUI or CLI, you can specify the IP addresses of the backup controllers, which allows the access points to fail over to controllers outside of the mobility group.

The following are some guidelines for configuring backup controllers:

- You can configure primary and secondary backup controllers (which are used if primary, secondary, or tertiary controllers are not specified or are not responsive) for all access points connected to the controller as well as various timers, including heartbeat timers and discovery request timers. To reduce the controller failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller.
- The access point maintains a list of backup controllers and periodically sends primary discovery requests to each entry on the list. When the access point receives a new discovery response from a controller, the backup controller list is updated. Any controller that fails to respond to two consecutive primary discovery requests is removed from the list. If the access point's local controller fails, it chooses an available controller from the backup controller list in this order: primary, secondary, tertiary, primary backup, and secondary backup. The access point waits for a discovery response from the first available controller in the backup list and joins the controller if it receives a response within the time configured for the primary discovery request timer. If the time limit is reached, the access point assumes that the controller cannot be joined and waits for a discovery response from the next available controller in the list.

- When an access point's primary controller comes back online, the access point disassociates from the backup controller and reconnects to its primary controller. The access point falls back only to its primary controller and not to any available secondary controller for which it is configured. For example, if an access point is configured with primary, secondary, and tertiary controllers, it fails over to the tertiary controller when the primary and secondary controllers become unresponsive. If the secondary controller comes back online while the primary controller is down, the access point does not fall back to the secondary controller and stays connected to the tertiary controller. The access point waits until the primary controller comes back online to fall back from the tertiary controller to the primary controller. If the tertiary controller fails and the primary controller is still down, the access point then falls back to the available secondary controller.

Restrictions for Configuring Backup Controllers

- You can configure the fast heartbeat timer only for access points in local and FlexConnect modes.

Configuring Backup Controllers (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the Global Configuration page.

Step 2 From the Local Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for access points in local mode or choose **Disable** to disable this timer. The default value is Disable.

Step 3 If you chose Enable in Step 2, enter the Local Mode AP Fast Heartbeat Timeout text box to configure the fast heartbeat timer for access points in local mode. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.
The range for the AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 (inclusive) for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

Step 4 From the FlexConnect Mode AP Fast Heartbeat Timer State drop-down list, choose **Enable** to enable the fast heartbeat timer for FlexConnect access points or choose **Disable** to disable this timer. The default value is Disable.

Step 5 If you enable FlexConnect fast heartbeat, enter the FlexConnect Mode AP Fast Heartbeat Timeout value in the FlexConnect Mode AP Fast Heartbeat Timeout text box. Specifying a small heartbeat interval reduces the amount of time it takes to detect a controller failure.
The range for the FlexConnect Mode AP Fast Heartbeat Timeout value for Cisco Flex 7500 Controllers is 10–15 (inclusive) and is 1–10 for other controllers. The default value for the heartbeat timeout for Cisco Flex 7500 Controllers is 10. The default value for other controllers is 1 second.

Step 6 In the AP Primary Discovery Timeout text box, a value between 30 and 3600 seconds (inclusive) to configure the access point primary discovery request timer. The default value is 120 seconds.

Step 7 If you want to specify a primary backup controller for all access points, enter the IPv4/IPv6 address of the primary backup controller in the Back-up Primary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Primary Controller Name text box.
Note The default value for the IP address is 0.0.0.0, which disables the primary backup controller.

Step 8 If you want to specify a secondary backup controller for all access points, enter the IPv4/IPv6 address of the secondary backup controller in the Back-up Secondary Controller IP Address (IPv4/IPv6) text box and the name of the controller in the Back-up Secondary Controller Name text box.

Note The default value for the IP address is 0.0.0.0, which disables the secondary backup controller.

Step 9 Click **Apply** to commit your changes.

Step 10 Configure primary, secondary, and tertiary backup controllers for a specific access point as follows:

a) Choose **Access Points** > **All APs** to open the All APs page.
b) Click the name of the access point for which you want to configure primary, secondary, and tertiary backup controllers.
c) Choose the **High Availability** tab to open the All APs > Details for (High Availability) page.
d) If desired, enter the name and IP address of the primary controller for this access point in the Primary Controller text boxes.

Note Entering an IP address for the backup controller is optional in this step and the next two steps. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. The controller name and IP address must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

e) If desired, enter the name and IP address of the secondary controller for this access point in the Secondary Controller text boxes.
f) If desired, enter the name and IP address of the tertiary controller for this access point in the Tertiary Controller text boxes.
g) Click **Apply** to commit your changes.

Step 11 Click **Save Configuration** to save your changes.

Configuring Backup Controllers (CLI)

Step 1 Configure a primary controller for a specific access point by entering this command:
config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

Note The *controller_ip_address* parameter in this command and the next two commands is optional. If the backup controller is outside the mobility group to which the access point is connected (the primary controller), then you need to provide the IP address of the primary, secondary, or tertiary controller, respectively. In each command, the *controller_name* and *controller_ip_address* must belong to the same primary, secondary, or tertiary controller. Otherwise, the access point cannot join the backup controller.

Step 2 Configure a secondary controller for a specific access point by entering this command:
config ap secondary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 3 Configure a tertiary controller for a specific access point by entering this command:
config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

Step 4 Configure a primary backup controller for all access points by entering this command:
config advanced backup-controller primary *system name ip_addr*

Note This command is valid for both IPv4 and IPv6

Step 5 Configure a secondary backup controller for all access points by entering this command:
config advanced backup-controller secondary *system name ip_addr*

Note To delete a primary or secondary backup controller entry, enter *0.0.0.0* for the controller IPv4/IPv6 address.

Note This command is valid for both IPv4 and IPv6

Step 6 Enable or disable the fast heartbeat timer for local or FlexConnect access points by entering this command:
config advanced timers ap-fast-heartbeat {**local** | **flexconnect** | **all**} {**enable** | **disable**} *interval*

where **all** is both local and FlexConnect access points, and *interval* is a value between 1 and 10 seconds (inclusive). Specifying a small heartbeat interval reduces the amount of time that it takes to detect a controller failure. The default value is disabled.Configure the access point heartbeat timer by entering this command:

config advanced timers ap-heartbeat-timeout *interval*

where *interval* is a value between 1 and 30 seconds (inclusive). This value should be at least three times larger than the fast heartbeat timer. The default value is 30 seconds.

Caution Do not enable the fast heartbeat timer with the high latency link. If you have to enable the fast heartbeat timer, the timer value must be greater than the latency.

Step 7 Configure the access point primary discovery request timer by entering this command:
config advanced timers ap-primary-discovery-timeout *interval*

where *interval* is a value between 30 and 3600 seconds. The default value is 120 seconds.

Step 8 Configure the access point discovery timer by entering this command:
config advanced timers ap-discovery-timeout *interval*

where *interval* is a value between 1 and 10 seconds (inclusive). The default value is 10 seconds.

Step 9 Configure the 802.11 authentication response timer by entering this command:
config advanced timers auth-timeout *interval*

where *interval* is a value between 5 and 600 seconds (inclusive). The default value is 10 seconds.

Step 10 Save your changes by entering this command:
save config

Step 11 See an access point's configuration by entering these commands:

- **show ap config general** *Cisco_AP*
- **show advanced backup-controller**
- **show advanced timers**

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv4:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP5
Country code..................................... US  - United States
Regulatory Domain allowed by Country.............. 802.11bg:-AB    802.11a:-AB
AP Country code.................................. US  - United States
AP Regulatory Domain............................. 802.11bg:-A    802.11a:-N
Switch Port Number .............................. 1
MAC Address...................................... 00:13:80:60:48:3e
```

```
IP Address Configuration..................... DHCP
IP Address................................... 1.100.163.133
...
Primary Cisco Switch Name.................... 1-5508
Primary Cisco Switch IP Address.............. 2.2.2.2
Secondary Cisco Switch Name.................. 1-4404
Secondary Cisco Switch IP Address............ 2.2.2.2
Tertiary Cisco Switch Name................... 2-4404
Tertiary Cisco Switch IP Address............. 1.1.1.4
...
```

Information similar to the following appears for the **show ap config general** *Cisco_AP* command for Primary Cisco Switch IP Address using IPv6:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP6
Country code..................................... US - United States
Regulatory Domain allowed by Country............. 802.11bg:-A 802.11a:-A
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 13
MAC Address...................................... 44:2b:03:9a:9d:30
IPv6 Address Configuration....................... DHCPv6
IPv6 Address..................................... 2001:9:5:96:295d:3b2:2db2:9b47
IPv6 Prefix Length............................... 128
Gateway IPv6 Addr................................ fe80::6abd:abff:fe8c:764a
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1473
Telnet State..................................... Globally Disabled
Ssh State........................................ Globally Disabled
Cisco AP Location................................ _5500
Cisco AP Floor Label............................. 0
Cisco AP Group Name.............................. IPv6-Same_VLAN
Primary Cisco Switch Name........................ Maulik_WLC_5500-HA
Primary Cisco Switch IP Address.................. 2001:9:5:95::11
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv4:

```
AP primary Backup Controller .................... controller1 10.10.10.10
AP secondary Backup Controller ................ 0.0.0.0
```

Information similar to the following appears for the **show advanced backup-controller** command when configured using IPv6:

```
AP primary Backup Controller .................... WLC_5500-2 fd09:9:5:94::11
AP secondary Backup Controller .................. vWLC 9.5.92.11
```

Information similar to the following appears for the **show advanced timers** command:

```
Authentication Response Timeout (seconds)........ 10
```

```
Rogue Entry Timeout (seconds)..................... 1300
AP Heart Beat Timeout (seconds)................... 30
AP Discovery Timeout (seconds).................... 10
AP Local mode Fast Heartbeat (seconds)........... 10 (enable)
AP flexconnect mode Fast Heartbeat (seconds)..... disable
AP Primary Discovery Timeout (seconds)........... 120
```

Configuring High Availability

This section describes how to configure high availability.

Information About High Availability

High availability (HA) in controllers allows you to reduce the downtime of the wireless networks that occurs due to the failover of controllers.

A 1:1 (Active:Standby-Hot) stateful switchover of access points (AP SSO) is supported. In an HA architecture, one controller is configured as the primary controller and another controller as the secondary controller.

After you enable HA, the primary and secondary controllers are rebooted. During the boot process, the role of the primary controller is negotiated as active and the role of the secondary controller as standby-hot. After a switchover, the secondary controller becomes the active controller and the primary controller becomes the standby-hot controller. After subsequent switchovers, the roles are interchanged between the primary and the secondary controllers. The reason for switchovers are either because of manual trigger, or a controller, or network failure.

During an AP SSO, all the AP sessions statefully switch over and all the clients are deauthenticated and reassociated with the new active controller except for the locally switched clients in the FlexConnect mode.

The standby-hot controller continuously monitors the health of the active controller through a direct wired connection over a dedicated redundancy port. Both the controllers share the same configurations, including the IP address of the management interface.

Before you enable HA, ensure that both the controllers are physically connected through the redundant port using an Ethernet cable. Also, ensure that the uplink is connected to an infrastructure switch and that the gateway is reachable from both the controllers.

In HA architecture, the redundancy port and redundant management interfaces have been introduced.

ACL and NAT IP configurations are synchronized to the HA standby controller when these parameters are configured before HA pair-up. If the NAT IP is set on the management interface, the access point sets the AP manager IP address as the NAT IP address. This issue is seen only when the NAT IP address and ACL are set on the management interface before you enable high availability.

The following are some guidelines for high availability:

- We recommend that you do not pair two controllers of different hardware models. If they are paired, the higher controller model becomes the active controller and the other controller goes into maintenance mode.

- We recommend that you do not pair two controllers on different controller software releases. If they are paired, the controller with the lower redundancy management address becomes the active controller and the other controller goes into maintenance mode.
- All download file types, such as image, configuration, web-authentication bundle, and signature files–are downloaded on the active controller first and then pushed to the standby-hot controller.
- Certificates should be downloaded separately on each controller before they are paired.
- You can upload file types such as configuration files, event logs, crash files, and so on, from the standby-hot controller using the GUI or CLI of the active controller. You can also specify a suffix to the filename to identify the uploaded file.
- To perform a peer upload, use the service port. In a management network, you can also use the redundancy management interface (RMI) that is mapped to the redundancy port or RMI VLAN, or both, where the RMI is the same as the management VLAN. Note that the RMI and the redundancy port should be in two separate Layer2 VLANs, which is a mandatory configuration.
- If the controllers cannot reach each other through the redundant port and the RMI, the primary controller becomes active and the standby-hot controller goes into the maintenance mode.

Note To achieve HA between two Cisco Wireless Services Module 2 (WiSM2) platforms, the controllers should be deployed on a single chassis, or on multiple chassis using a virtual switching system (VSS) and extending a redundancy VLAN between the multiple chassis.

Note A redundancy VLAN should be a nonroutable VLAN in which a Layer 3 interface should not be created for the VLAN, and the interface should be allowed on the trunk port to extend an HA setup between multiple chassis. Redundancy VLAN should be created like any other data VLAN on Cisco IOS-based switching software. A redundancy VLAN is connected to the redundant port on Cisco WiSM2 through the backplane. It is not necessary to configure the IP address for the redundancy VLAN because the IP address is automatically generated. Also, ensure that the redundancy VLAN is not the same as the management VLAN.

Note When the RMIs for two controllers that are a pair, and that are mapped to same VLAN and connected to same Layer3 switch stop working, the standby controller is restarted.

Note The " mobilityHaMac is out of range" xml message is seen during the active/standby second switch over in HA setup. This occurs if mobility HA mac field is more than 128.

- When HA is enabled, the standby controller always uses RMI and all the other interfaces, dynamic and management, are invalid. A ping must only accept RMI as source and not other interfaces.
- When HA is enabled, ensure that you do not use the backed-up image. If this image is used, the HA feature might not work as expected:

- The service port and route information that is configured is lost after you enable SSO. You must configure the service port and route information again after you enable SSO. You can configure the service port and route information for the standby-hot controller using the **peer-service-port** and **peer-route** commands.
- For Cisco WiSM2, service port reconfigurations are required after you enable redundancy. Otherwise, Cisco WiSM2 might not be able to communicate with the supervisor. We recommend that you enable DHCP on the service port before you enable redundancy.
- We recommend that you do not use the **reset** command on the standby-hot controller directly. If you use this, unsaved configurations will be lost.

- We recommend that you enable link aggregation configuration on the controllers before you enable the port channel in the infrastructure switches.
- All the configurations that require reboot of the active controller results in the reboot of the standby-hot controller.
- The Ignore AP list is not synchronized from the active controller to the standby-hot controller. The list is relearned through SNMP messages from Cisco Prime Infrastructure after the standby-hot controller becomes active.
- In Release 7.3.x, AP SSO is supported, but client SSO is not supported, which means that after an HA setup that uses Release 7.3.x encounters a switchover, all the clients associated with the controller are deauthenticated and forced to reassociate.
- You must manually configure the mobility MAC address on the then active controller post switchover, when a peer controller has a controller software release that is prior to Release 7.2.

Redundancy Management Interface

The active and standby-hot controllers use the RMI to check the health of the peer controller and the default gateway of the management interface through network infrastructure.

The RMI is also used to send notifications from the active controller to the standby-hot controller if a failure or manual reset occurs. The standby-hot controller uses the RMI to communicate to the syslog, NTP/SNTP server, FTP, and TFTP server.

It is mandatory to configure the IP addresses of the Redundancy Management Interface and the Management Interface in the same subnet on both the primary and secondary controllers.

Redundancy Port

The redundancy port is used for configuration, operational data synchronization, and role negotiation between the primary and secondary controllers.

The redundancy port checks for peer reachability by sending UDP keepalive messages every 100 milliseconds (default frequency) from the standby-hot controller to the active controller. If a failure of the active controller occurs, the redundancy port is used to notify the standby-hot controller.

If an NTP/SNTP server is not configured, the redundancy port performs a time synchronization from the active controller to the standby-hot controller.

In Cisco WiSM2, the redundancy VLAN must be configured on the Cisco Catalyst 6000 Supervisor Engine because there is no physical redundancy port available on Cisco WiSM2.

The redundancy port and the redundancy VLAN in Cisco WiSM2 are assigned an automatically generated IP address in which the last two octets are obtained from the last two octets of the RMI. The first two octets

are always 169.254. For example, if the IP address of the RMI is 209.165.200.225, the IP address of the redundancy port is 169.254.200.225.

Restrictions on High Availability

- We recommend that you do not disable LAG physical ports when HA SSO is enabled.
-
- HA is not supported on the Cisco 2500 Series and Cisco Virtual Wireless LAN Controllers.
- When you configure the controller for AP SSO, the Cisco 600 Series OfficeExtend Access Points are not supported.
- In an HA environment using FlexConnect locally switched clients, the client information might not show the username. To get details about the client, you must use the MAC address of the client. This restriction does not apply to FlexConnect centrally switched clients or central (local) mode clients.
- It is not possible to access the Cisco WiSM2 GUI through the service interface when you have enabled HA. The workaround is to create a service port interface again after HA is established.
- In an HA environment, an upgrade from an LDPE image to a non-LDPE image is not supported.
- It is not possible to pair two primary controllers or two secondary controllers.
- Standby controllers are unavailable on the APs connected switch port
- An HA-SKU controller with an evaluation license cannot become a standby controller. However, an HA-SKU controller with zero license can become a standby controller.
- Service VLAN configuration is lost when moving from HA mode to non-HA mode and vice versa. You should configure the service IP address manually again.
- The following scenario is not supported: The primary controller has the management address and the redundancy management address in the same VLAN, and the secondary controller has the management address in the same VLAN as the primary one, and the redundancy management address in a different VLAN.
- The following is a list of some software upgrade scenarios:
    - A software upgrade on the active controller ensures the upgrade of the standby-hot controller.
    - An in-service upgrade is not supported. Therefore, you should plan your network downtime before you upgrade the controllers in an HA environment.
    - Rebooting the active controller after a software upgrade also reboots the standby-hot controller.
    - If both active and standby-hot controllers have different software releases in the backup, and if you enter the **config boot backup** command in the active controller, both the controllers reboot with their respective backup images breaking the HA pair due to a software mismatch.
    - A schedule reset applies to both the controllers in an HA environment. The peer controller reboots a minute before the scheduled time expires on the active controller.
    - You can reboot the standby-hot controller from the active controller by entering the **reset peer-system** command if the scheduled reset is not planned. If you reset only the standby-hot controller with this command, any unsaved configurations on the standby-hot controller is lost. Therefore, ensure that you save the configurations on the active controller before you reset the standby-hot controller.

- A preimage download is reinitiated if an SSO is triggered at the time of the image transfer.
- Only **debug** and **show** commands are allowed on the standby-hot controller.

- It is not possible to access the standby-hot controller through the controller GUI, Cisco Prime Infrastructure, or Telnet. You can access the standby-hot controller only on its console.
- When a failover occurs, the standby controller must be in a standby-hot state and the redundant port in a terminal state in SSO for successful switchover to occur.
- To enable or disable LAG, you must disable HA.

Note If LAG is disabled and both primary and backup ports are connected to the management interface and if the primary port becomes nonoperational, a switchover might occur because the default gateway is not reachable and backup port failover might exceed 12 seconds.

- Pairwise Master Key (PMK) cache synchronization is not supported on FlexConnect local-authenticated clients.
- You cannot change the NAT address configuration of the management interface when the controllers are in redundancy mode. To enable NAT address configuration on the management interface, you must remove the redundancy configuration first, make the required changes on the primary controller, and then reenable the redundancy configuration on the same controller.
- After you enable SSO, you must access both the standby and active controller using:
  - The console connection
  - SSH facility on the service port
  - SSH facility on the redundant management interface

Note While SSO is enabled, you can not access both the standby and active controller either using the web UI/the telnet facility or using Cisco Prime Infrastructure/Prime NCS on the service port.

- Synchronization of bulk configurations is supported only for the configurations that are stored in XMLs. Scheduled reboot is a configuration that is not stored in XMLs or Flash. Therefore, the scheduled reboot configuration is not included in the synchronization of bulk configurations.
- When a switchover occurs, the controller does not synchronize the information on DHCP dirty bit from the active to standby controller even when DHCP dirty bit is set on the active controller. After a switchover, the controller populates the DHCP dirty bit based on the client DHCP retries.
- If you are using Cisco WiSM2, we recommend that you use the following release versions of Cisco IOS on Cisco Catalyst 6500 Series Supervisor Engine 2T:
  - 15.1(02)SY
  - 15.1(01)ICB40.1
  - 15.1(01)ICB29.36

- 15.1(01)ICB29.1
- 15.1(01)IC66.25
- 15.1(01)IB273.72

Configuring High Availability (GUI)

Before You Begin

Ensure that the management interfaces of both controllers are in the same subnet. You can verify this on the GUI of both the controllers by choosing **Controllers > Interfaces** and viewing the IP addresses of the management interface.

Step 1 On the GUI of both the controllers, choose **Controller > Redundancy > Global Configuration**. The **Global Configuration** page is displayed.

Step 2 Enter the addresses of the controllers in the **Redundant Management IP** and the **Peer Redundant Management IP** text boxes.

Note Ensure that the Redundant Management Interface IP address of one controller is the same as the Redundant Management Interface IP address of the peer controller.

Step 3 From the **Redundant Unit** drop-down list, choose one of the controllers as primary and the other as secondary.

Step 4 On the GUI of both the controllers, set the **SSO** to Enabled state.

Note After you enable an SSO, the service port peer IP address and the service port netmask appear on the configuration page. Note that the service port peer IP address and the netmask can be pushed to the peer only if the HA peer is available and operational. When you enable high availability, you do not have to configure the service port peer IP address and the service port netmask parameters. You must configure the parameters only when the HA peer is available and operational. After you enable SSO, both the controllers are rebooted. During the reboot process, the controllers negotiate the redundancy role through the redundant port based on the configuration. The primary controller becomes the active controller and the secondary controller becomes the standby controller.

Step 5 (Optional) When the HA pair becomes available and operational, you can configure the peer service port IP address and the netmask when the service port is configured as static. If you enable DHCP on the service port, you do not have to configure these parameters on the **Global Configuration** page:

- **Service Port Peer IP—**IP address of the service port of the peer controller.
- **Service Port Peer Netmask—**Netmask of the service port of the peer controller.
- **Mobility MAC Address—**A common MAC address for the active and standby controllers that is used in the mobility protocol. If an HA pair has to be added as a mobility member for a mobility group, the mobility MAC address (instead of the system MAC address of the active or standby controller) should be used. Normally, the mobility MAC address is chosen as the MAC address of the active controller and you do not have to manually configure this.
- **Keep Alive Timer—**The timer that controls how often the standby controller sends keepalive messages to the active controller. The valid range is between 100 to 1000 milliseconds.
- **Peer Search Timer—**The timer that controls how often the active controller sends peer search messages to the standby controller. The valid range is between 60 to 300 seconds.

After you enable the high availability and pair the controllers, there is only one unified GUI to manage the HA pair through the management port. GUI access through the service port is not feasible for both the active and standby controllers. The standby controller can be managed only through the console or the service port.

Only Telnet and SSH sessions are allowed through the service port of the active and standby controllers.

Step 6 Click **Apply**.

Step 7 Click **Save Configuration**.

Step 8 View the redundancy status of the HA pair by choosing **Monitor > Redundancy > Summary**.
The **Redundancy Summary** page is displayed.

Step 9 Follow these steps to configure the peer network route:

a) Choose **Controller** > **Redundancy** > **Peer Network Route**.
The **Network Routes Peer** page is displayed.

This page provides a summary of the existing service port network routes of the peer controller to network or element management systems on a different subnet. You can view the IP address, IP netmask, and gateway IP address.

b) To create a new peer network route, click **New**.

c) Enter the IP address, IP netmask, and the Gateway IP address of the route.

d) Click **Apply**.

Configuring High Availability (CLI)

Before You Begin

Ensure that the management interfaces of both controllers are in the same subnet.

To configure high availability in controllers, you must:

- Configure a local-redundancy IP address and a peer-redundancy management IP address by entering this command:
config interface address redundancy-management *ip-addr1* **peer-redundancy-management** *ip-addr2*
- Configure the role of a controller by entering this command:
config redundancy unit {**primary** | **secondary**}
- Configure the redundancy mode by entering this command:
config redundancy mode {**sso** | **none**}

Note Both controllers reboot and then negotiate the roles of active and standby-hot controllers.

- Configure the route configurations of the standby controller by entering this command:
config redundancy peer-route {**add** *network-ip-addr ip-mask* | **delete** *network-ip-addr*}

Note This command can be run only if the HA peer controller is available and operational.

- Configure a mobility MAC address by entering this command:
  config redundancy mobilitymac *mac-addr*

Note This command can be run only when SSO is disabled.

- Configure the IP address and netmask of the peer service port of the standby controller by entering this command:
  config redundancy interface address peer-service-port *ip-address netmask*

  This command can be run only if the HA peer controller is available and operational.
- Initiate a manual switchover by entering this command:
  redundancy force-switchover

Note Execute this command only when you require a manual switchover.

- Configure a redundancy timer by entering this command:
  config redundancy timer {**keep-alive-timer** *time-in-milliseconds* | **peer-search-timer** *time-in-seconds*}
- View the status of redundancy by entering this command:
  show redundancy summary
- View information about the Redundancy Management Interface by entering this command:
  show interface detailed redundancy-management
- View information about the redundancy port by entering this command:
  show interface detailed redundancy-port
- Reboot a peer controller by entering this command:
  reset peer-system
- Start the upload of file types, such as configuration, event logs, crash files, and so on from the standby-hot controller by entering this command on the active controller:
  transfer upload peer-start
- Debug the redundancy modules by entering these commands:

Note Ensure that SSO is enabled to use these debug commands. Enter **config redundancy mode SSO** command to enable SSO.

debug redundancy {**infra** | **facilitator** | **transport** | **keepalive** | **gw-reachability** | **config-sync** | **ap-sync** | **client-sync** | **mobility**}

- **infra—**Configures debug of Redundancy Infra Module
- **facilitator—**Configures debug of Redundancy Facilitator Module
- **transport—**Configures debug of Redundancy Transport Module
- **keepalive—**Configures debug of Redundancy Keepalive Module
- **gw-reachability—**Configures debug of Redundancy Gw-reachability Module

- **config-sync—**Configures debug of Redundancy Config-Sync Module
- **ap-sync—**Configures debug of Redundancy AP-Sync Module
- **client-sync—**Configures debug of Redundancy Client-Sync Module
- **mobility—**Configures debug of Redundancy Mobility Module

Configuring Failover Priority for Access Points

Information About Configuring Failover Priority for Access Points

Each controller has a defined number of communication ports for access points. When multiple controllers with unused access point ports are deployed on the same network and one controller fails, the dropped access points automatically poll for unused controller ports and associate with them.

The following are some guidelines for configuring failover priority for access points:

- You can configure your wireless network so that the backup controller recognizes a join request from a higher-priority access point and if necessary disassociates a lower-priority access point as a means to provide an available port.
- Failover priority is not in effect during the regular operation of your wireless network. It takes effect only if there are more association requests after a controller failure than there are available backup controller ports.
- To configure this feature, you must enable failover priority on your network and assign priorities to the individual access points.
- By default, all access points are set to priority level 1, which is the lowest priority level. Therefore, you need to assign a priority level only to those access points that warrant a higher priority.

Configuring Failover Priority for Access Points (GUI)

Step 1 Choose **Wireless > Access Points > Global Configuration** to open the Global Configuration page.

Step 2 From the Global AP Failover Priority drop-down list, choose **Enable** to enable access point failover priority or choose **Disable** to disable this feature and turn off any access point priority assignments. The default value is Disable.

Step 3 Click **Apply** to commit your changes.

Step 4 Click **Save Configuration** to save your changes.

Step 5 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 6 Click the name of the access point for which you want to configure failover priority.

Step 7 Choose the **High Availability** tab. The All APs > Details for (High Availability) page appears.

Step 8 From the AP Failover Priority drop-down list, choose one of the following options to specify the priority of the access point:

- **Low—**Assigns the access point to the level 1 priority, which is the lowest priority level. This is the default value.
- **Medium—**Assigns the access point to the level 2 priority.
- **High—**Assigns the access point to the level 3 priority.
- **Critical—**Assigns the access point to the level 4 priority, which is the highest priority level.

Step 9 Click **Apply** to commit your changes.

Step 10 Click **Save Configuration** to save your changes.

Configuring Failover Priority for Access Points (CLI)

Step 1 Enable or disable access point failover priority by entering this command:
config network ap-priority {**enable** | **disable**}

Step 2 Specify the priority of an access point by entering this command:
config ap priority {**1** | **2** | **3** | **4**} *Cisco_AP*

where 1 is the lowest priority level and 4 is the highest priority level. The default value is 1.

Step 3 Enter the **save config** command to save your changes.

Viewing Failover Priority Settings (CLI)

- Confirm whether access point failover priority is enabled on your network by entering this command:

  show network summary

  Information similar to the following appears:

```
RF-Network Name............................. mrf
Web Mode.................................... Enable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Shell (ssh).......................... Enable
Telnet...................................... Enable
Ethernet Multicast Mode..................... Disable
Ethernet Broadcast Mode..................... Disable
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority.......................... Enabled

...
```

- See the failover priority for each access point by entering this command:

show ap summary

Information similar to the following appears:

```
Number of APs.................................. 2
Global AP User Name............................ user
Global AP Dot1x User Name...................... Not Configured

AP Name  Slots  AP Model           Ethernet MAC       Location   Port Country Priority
-------  -----  ------------------ -----------------  ---------  ---- ------- -------
ap:1252  2      AIR-LAP1252AG-A-K9 00:1b:d5:13:39:74  hallway 6  1    US      1
ap:1121  1      AIR-LAP1121G-A-K9  00:1b:d5:a9:ad:08  reception  1    US      3
```

To see the summary of a specific access point, you can specify the access point name. You can also use wildcard searches when filtering for access points.

Configuring Access Point Retransmission Interval and Retry Count

Information About Configuring the AP Retransmission Interval and Retry Count

The controller and the APs exchange packets using the CAPWAP reliable transport protocol. For each request, a response is defined. This response is used to acknowledge the receipt of the request message. Response messages are not explicitly acknowledged; therefore, if a response message is not received, the original request message is retransmitted after the retransmit interval. If the request is not acknowledged after a maximum number of retransmissions, the session is closed and the APs reassociate with another controller.

Restrictions for Access Point Retransmission Interval and Retry Count

- You can configure the retransmission intervals and retry count both at a global as well as a specific access point level. A global configuration applies these configuration parameters to all the access points. That is, the retransmission interval and the retry count are uniform for all access points. Alternatively, when you configure the retransmission level and retry count at a specific access point level, the values are applied to that particular access point. The access point specific configuration has a higher precedence than the global configuration.
- Retransmission intervals and the retry count do not apply for mesh access points.

Configuring the AP Retransmission Interval and Retry Count (GUI)

You can configure the retransmission interval and retry count for all APs globally or a specific AP.

Step 1 To configure the controller to set the retransmission interval and retry count globally using the controller GUI, follow these steps:

a) Choose **Wireless > Access Points > Global Configuration**.

b) Choose one of the following options under the AP Transmit Config Parameters section:

- **AP Retransmit Count—**Enter the number of times you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval—**Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

c) Click **Apply**.

Step 2 To configure the controller to set the retransmission interval and retry count for a specific access point, follow these steps:

a) Choose **Wireless > Access Points > All APs**.
b) Click on the AP Name link for the access point on which you want to set the values.
The **All APs > Details** page appears.
c) Click the **Advanced Tab** to open the advanced parameters page.
d) Choose one of the following parameters under the AP Transmit Config Parameters section:

- **AP Retransmit Count—**Enter the number of times that you want the access point to retransmit the request to the controller. This parameter can take values between 3 and 8.
- **AP Retransmit Interval—**Enter the time duration between the retransmission of requests. This parameter can take values between 2 and 5.

e) Click **Apply**.

Configuring the Access Point Retransmission Interval and Retry Count (CLI)

You can configure the retransmission interval and retry count for all access points globally or a specific access point.

- Configure the retransmission interval and retry count for all access points globally by entering the this command:

  config ap retransmit {**interval** | **count**} *seconds* **all**

  The valid range for the **interval** parameter is between 3 and 8. The valid range for the **count** parameter is between 2 and 5.

- Configure the retransmission interval and retry count for a specific access point, by entering this command:

  config ap retransmit {**interval** | **count**} *seconds Cisco_AP*

  The valid range for the **interval** parameter is between 3 and 8. The valid range for the **count** parameter is between 2 and 5.

- See the status of the configured retransmit parameters on all or specific APs by entering this command:

  show ap retransmit all

Note Because retransmit and retry values cannot be set for access points in mesh mode, these values are displayed as N/A (not applicable).

- See the status of the configured retransmit parameters on a specific access point by entering this command:

  show ap retransmit *Cisco_AP*

Configuring Country Codes

Information About Configuring Country Codes

Controllers and access points are designed for use in many countries with varying regulatory requirements. The radios within the access points are assigned to a specific regulatory domain at the factory (such as -E for Europe), but the country code enables you to specify a particular country of operation (such as FR for France or ES for Spain). Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations.

The following are some guidelines for configuring country codes:

- Generally, you configure one country code per controller, the one matching the physical location of the controller and its access points. However, you can configure more than one country code per Cisco WLC. Prior to Release 8.2, you could configure up to 20 country codes per Cisco WLC; from Release 8.2 onwards, you can configure up to 110 country codes per Cisco WLC. This multiple-country support enables you to manage access points in various countries from a single Cisco WLC.
- Although the controller supports different access points in different regulatory domains (countries), it requires all radios in a single access point to be configured for the same regulatory domain. For example, you should not configure a Cisco 1231 access point's 802.11b/g radio for the US (-A) regulatory domain and its 802.11a radio for the Great Britain (-E) regulatory domain. Otherwise, the controller allows only one of the access point's radios to turn on, depending on which regulatory domain you selected for the access point on the controller. Therefore, make sure that the same country code is configured for both of the access point's radios.

  For a complete list of country codes supported per product, see http://tools.cisco.com/cse/prdapp/jsp/externalsearch.do?action=externalsearch&page=EXTERNAL_SEARCH

  or

  http://www.cisco.com/c/en/us/products/collateral/wireless/access-points/product_data_sheet0900aecd80537b6a.html
- When the multiple-country feature is being used, all controllers that are going to join the same RF group must be configured with the same set of countries, configured in the same order.
- When multiple countries are configured and the RRM auto-RF feature is enabled, the RRM assigns the channels that are derived by performing a union of the allowed channels per the AP country code. The APs are assigned channels by the RRM based on their PID country code. APs are only allowed to use legal frequencies that match their PID country code. Ensure that your AP's country code is legal in the country that it is deployed.
- The country list configured on the RF group leader determines what channels the members would operate on. This list is independent of what countries have been configured on the RF group members.

Information About Japanese Country Codes

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller
- J3—Uses the -U frequencies but allows -U, -P and -Q (other than 1550/1600/2600/3600) radios to join the WLC
- J4—Allows 2.4G JPQU and 5G PQU to join the controller.

Note The 1550, 1600, 2600, and 3600 APs require J4.

See the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

Restrictions for Configuring Country Codes

- The access point can only operate on the channels for the countries that they are designed for.

Note If an access point was already set to a higher legal power level or is configured manually, the power level is limited only by the particular country to which that access point is assigned.

Configuring Country Codes (GUI)

Step 1 Disable the 802.11 networks as follows:
a) Choose **Wireless** > **802.11a/n** > **Network**.
b) Unselect the **802.11a Network Status** check box.
c) Click **Apply**.
d) Choose **Wireless** > **802.11a/n** > **Network**.
e) Unselect the **802.11b/g Network Status** check box.
f) Click **Apply**.

Step 2 Choose **Wireless** > **Country** to open the Country page.

Step 3 Select the check box for each country where your access points are installed. If you selected more than one check box, a message appears indicating that RRM channels and power levels are limited to common channels and power levels.

Step 4 Click **OK** to continue or **Cancel** to cancel the operation.

Step 5 Click **Apply**.

If you selected multiple country codes in *Step 3*, each access point is assigned to a country.

Step 6 See the default country chosen for each access point and choose a different country if necessary as follows:

Note If you remove a country code from the configuration, any access points currently assigned to the deleted country reboot and when they rejoin the controller, they get re-assigned to one of the remaining countries if possible.

a) Perform one of the following:

- Leave the 802.11 networks disabled.
- Reenable the 802.11 networks and then disable only the access points for which you are configuring a country code. To disable an access point, choose **Wireless** > **Access Points** > **All APs**, click the link of the desired access point, choose **Disable** from the Status drop-down list, and click **Apply**.

b) Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.
c) Click the link for the desired access point.
d) Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.
The default country for this access point appears in the Country Code drop-down list.
e) If the access point is installed in a country other than the one shown, choose the correct country from the drop-down list. The box contains only those country codes that are compatible with the regulatory domain of at least one of the access point's radios.
f) Click **Apply**.
g) Repeat these steps to assign all access points joined to the controller to a specific country.
h) Reenable any access points that you disabled in *Step a*.

Step 7 Reenable the 802.11 networks if you did not enable them in *Step 6*.

Step 8 Click **Save Configuration**.

Configuring Country Codes (CLI)

Step 1 See a list of all available country codes by entering this command:
show country supported

Step 2 Disable the 802.11 networks by entering these commands:
config 802.11a disable network

config 802.11b disable network

Step 3 Configure the country codes for the countries where your access points are installed by entering this command:
config country *code1*[,*code2*,*code3*,...]

If you are entering more than one country code, separate each by a comma (for example, **config country US,CA,MX**).

Step 4 Enter **Y** when prompted to confirm your decision.

Step 5 Verify your country code configuration by entering this command:
show country

Step 6 See the list of available channels for the country codes configured on your controller by entering this command:
show country channels

Step 7 Save your changes by entering this command:
save config

Step 8 See the countries to which your access points have been assigned by entering this command:
To see a summary of specific access point you can specify the access point name. You can also use wildcard searches when filtering for access points.

show ap summary

Step 9 If you entered multiple country codes in *Step 3*, follow these steps to assign each access point to a specific country:

a) Perform one of the following:

- Leave the 802.11 networks disabled.
- Reenable the 802.11 networks and then disable only the access points for which you are configuring a country code. To Reenable the networks, enter this command:

  config 802.11{**a** | **b**} **enable network**

  To disable an access point, enter this command:

  config ap disable *ap_name*

b) To assign an access point to a specific country, enter this command:
config ap country *code* {*ap_name* | **all**}

Make sure that the country code you choose is compatible with the regulatory domain of at least one of the access point's radios.

Note If you enabled the networks and disabled some access points and then run the **config ap country** *code* **all** command, the specified country code is configured on only the disabled access points. All other access points are ignored.

c) To reenable any access points that you disabled in *Step a*, enter this command:
config ap enable *ap_name*

Step 10 If you did not reenable the 802.11 networks in *Step 9*, enter these commands to reenable them now:
config 802.11{**a** | **b**} **enable network**

Step 11 Save your changes by entering this command:
save config

Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

Information About Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

The Japanese government has changed its 5-GHz radio spectrum regulations. These regulations allow a text box upgrade of 802.11a 5-GHz radios. Japan allows three frequency sets:

- J52 = 34 (5170 MHz), 38 (5190 MHz), 42 (5210 MHz), 46 (5230 MHz)
- W52 = 36 (5180 MHz), 40 (5200 MHz), 44 (5220 MHz), 48 (5240 MHz)
- W53 = 52 (5260 MHz), 56 (5280 MHz), 60 (5300 MHz), 64 (5320 MHz)

Cisco has organized these frequency sets into the following regulatory domains:

- -J regulatory domain = J52
- -P regulatory domain = W52 + W53
- -U regulatory domain = W52

Regulatory domains are used by Cisco to organize the legal frequencies of the world into logical groups. For example, most of the European countries are included in the -E regulatory domain. Cisco access points are configured for a specific regulatory domain at the factory and, with the exception of this migration process, never change. The regulatory domain is assigned per radio, so an access point's 802.11a and 802.11b/g radios may be assigned to different domains.

Note Controllers and access points may not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase controllers and access points that match your country's regulatory domain.

The Japanese regulations allow the regulatory domain that is programmed into an access point's radio to be migrated from the -J domain to the -U domain. New access points for the Japanese market contain radios that are configured for the -P regulatory domain. -J radios are no longer being sold. In order to make sure that your existing -J radios work together with the new -P radios in one network, you need to migrate your -J radios to the -U domain.

Country codes define the channels that can be used legally in each country. These country codes are available for Japan:

- JP—Allows only -J radios to join the controller
- J2—Allows only -P radios to join the controller
- J3—Uses the -U frequencies but allows both -U and -P radios to join the controller
- J4—Allows 2.4G PQU and 5G JPQU to join the controller.

Note After migration, you need to use the J3 country code. If your controller is running software release 4.1 or later releases, you can use the multiple-country feature to choose both J2 and J3. You can manually configure your -P radios to use the channels not supported by J3.

If you are using controller software 7.0.98.0 or earlier releases, you must enable J2 and J4 for the Q radios.

See the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points* document for the list of channels and power levels supported by access points in the Japanese regulatory domains.

Restrictions for Migrating Access Points from the -J Regulatory Domain to the -U Regulatory Domain

- You can migrate only Cisco Aironet 1130, 1200, and 1240 lightweight access points that support the -J regulatory domain and Airespace AS1200 access points. Other access points cannot be migrated.
- You must have had one or more Japan country codes (JP, J2, or J3) configured on your controller at the time you last booted your controller.
- You must have at least one access point with a -J regulatory domain associated with your controller.
- You cannot migrate your access points from the -U regulatory domain back to the -J domain. The Japanese government has made reverse migration illegal.

Note You cannot undo an access point migration. Once an access point has been migrated, you cannot return to software release 4.0. Migrated access points will have nonfunctioning 802.11a radios under software release 4.0.

- The migration process cannot be performed using the controller GUI.

Migrating Access Points to the -U Regulatory Domain (CLI)

Step 1 Determine which access points in your network are eligible for migration by entering this command:
show ap migrate

Information similar to the following appears:

```
These 1 APs are eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9 ap1240 “J” Reg. Domain

No APs have already been migrated.
```

Step 2 Disable the 802.11a and 802.11b/g networks by entering these commands:
config 802.11a disable network

config 802.11b disable network

Step 3 Change the country code of the access points to be migrated to J3 by entering this command:
config country J3

Step 4 Wait for any access points that may have rebooted to rejoin the controller.

Step 5 Migrate the access points from the -J regulatory domain to the -U regulatory domain by entering this command:
config ap migrate j52w52 {**all** | *ap_name*}

Information similar to the following appears:

```
Migrate APs with 802.11A Radios in the "J" Regulatory Domain to the "U" Regulatory Domain.
The "J" domain allows J52 frequencies, the "U" domain allows W52 frequencies.
WARNING: This migration is permanent and is not reversible, as required by law.
WARNING: Once migrated the 802.11A radios will not operate with previous OS versions.
WARNING: All attached "J" radios will be migrated.
WARNING: All migrated APs will reboot.
WARNING: All migrated APs must be promptly reported to the manufacturer.
Send the AP list and your company name to: abc@cisco.com

This AP is eligible for migration:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9 ap1240

Begin to migrate Access Points from "J"(J52) to "U"(W52). Are you sure? (y/n)
```

Step 6 Enter **Y** when prompted to confirm your decision to migrate.

Step 7 Wait for all access points to reboot and rejoin the controller. This process may take up to 15 minutes, depending on access point. The AP1130, AP1200, and AP1240 reboot twice; all other access points reboot once.

Step 8 Verify migration for all access points by entering this command:
show ap migrate

Information similar to the following appears:

```
No APs are eligible for migration.

These 1 APs have already been migrated:
00:14:1c:ed:27:fe AIR-AP1242AG-J-K9 ap1240  "U" Reg. Domain
```

Step 9 Reenable the 802.11a and 802.11b/g networks by entering these commands:
config 802.11a enable network

config 802.11b enable network

Step 10 Send an e-mail with your company name and the list of access points that have been migrated to this e-mail address: migrateapj52w52@cisco.com. We recommend that you cut and paste the output from the **show ap migrate** command in Step 8 into the e-mail.

Using the W56 Band in Japan

The Japanese government is formally permitting wireless LAN use of the frequencies in the W56 band for 802.11a radios. The W56 band includes the following channels, frequencies, and power levels (in dBm):

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
100	5500	17	15

Channel	Frequency (MHz)	Maximum Power for AIR-LAP1132AG-Q-K9	Maximum Power for AIR-LAP1242AG-Q-K9
104	5520	17	15
108	5540	17	15
112	5560	17	15
116	5580	17	15
120	5600	17	15
124	5620	17	15
128	5640	17	15
132	5660	17	15
136	5680	17	15
140	5700	17	15

All of the channels in the W56 band require dynamic frequency selection (DFS). In Japan, the W56 band is subject to Japan's DFS regulations. Currently, only the new 1130 and 1240 series access point SKUs (with the -Q product code) support this requirement: AIR-LAP1132AG-Q-K9 and AIR-LAP1242AG-Q-K9.

To set up a network consisting of only -P and -Q access points, configure the country code to J2. To set up a network consisting of -P, -Q, and -U access points, configure the country code to J3.

Dynamic Frequency Selection

The Cisco UWN solution complies with regulations that require radio devices to use dynamic frequency selection (DFS) to detect radar signals and avoid interfering with them.

When a lightweight access point with a 5-GHz radio operates on one of the 15 channels listed in the table below, the controller to which the access point is associated automatically uses DFS to set the operating frequency.

When you manually select a channel for DFS-enabled 5-GHz radios, the controller checks for radar activity on the channel for 60 seconds. If there is no radar activity, the access point operates on the channel that you selected. If there is radar activity on the channel that you selected, the controller automatically selects a different channel, and after 30 minutes, the access point retries the channel.

Note After radar has been detected on a DFS-enabled channel, it cannot be used for 30 minutes.

Note The Rogue Location Detection Protocol (RLDP) and rogue containment are not supported on the channels listed in the table below.

Note The maximum legal transmit power is greater for some 5-GHz channels than for others. When the controller randomly selects a 5-GHz channel on which power is restricted, it automatically reduces transmit power to comply with power limits for that channel.

Table 3: DFS-Enabled 5-GHz Channels

52 (5260 MHz)	104 (5520 MHz)	124 (5620 MHz)
56 (5280 MHz)	108 (5540 MHz)	128 (5640 MHz)
60 (5300 MHz)	112 (5560 MHz)	132 (5660 MHz)
64 (5320 MHz)	116 (5580 MHz)	136 (5680 MHz)
100 (5500 MHz)	120 (5600 MHz)	140 (5700 MHz)

Using DFS, the controller monitors operating frequencies for radar signals. If it detects radar signals on a channel, the controller takes these steps:

- It changes the access point channel to a channel that has not shown radar activity within the last 30 minutes. (The radar event is cleared after 30 minutes.) The controller selects the channel at random.
- If the channel selected is one of the channels in the table above, it scans the new channel for radar signals for 60 seconds. If there are no radar signals on the new channel, the controller accepts client associations.
- It records the channel that showed radar activity as a radar channel and prevents activity on that channel for 30 minutes.
- It generates a trap to alert the network manager.

Optimizing RFID Tracking on Access Points

Information About Optimizing RFID Tracking on Access Points

To optimize the monitoring and location calculation of RFID tags, you can enable tracking optimization on up to four channels within the 2.4-GHz band of an 802.11b/g access point radio. This feature allows you to scan only the channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

You can use the controller GUI or CLI to configure the access point for monitor mode and to then enable tracking optimization on the access point radio.

Optimizing RFID Tracking on Access Points (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure monitor mode. The All APs > Details for page appears.

Step 3 From the AP Mode drop-down list, choose **Monitor**.

Step 4 Click **Apply**.

Step 5 Click **OK** when warned that the access point will be rebooted.

Step 6 Click **Save Configuration** to save your changes.

Step 7 Choose **Wireless** > **Access Points** > **Radios** > **802.11b/g/n** to open the 802.11b/g/n Radios page.

Step 8 Hover your cursor over the blue drop-down arrow for the desired access point and choose **Configure**. The 802.11b/g/n Cisco APs > Configure page appears.

Step 9 Disable the access point radio by choosing **Disable** from the Admin Status drop-down list and click **Apply**.

Step 10 Enable tracking optimization on the radio by choosing **Enable** from the Enable Tracking Optimization drop-down list.

Step 11 From the four Channel drop-down lists, choose the channels on which you want to monitor RFID tags.

Note You must configure at least one channel on which the tags will be monitored.

Step 12 Click **Apply**.

Step 13 Click **Save Configuration**.

Step 14 To reenable the access point radio, choose **Enable** from the Admin Status drop-down list and click **Apply**.

Step 15 Click **Save Configuration**.

Optimizing RFID Tracking on Access Points (CLI)

Step 1 Configure an access point for monitor mode by entering this command:
config ap mode monitor *Cisco_AP*

Step 2 When warned that the access point will be rebooted and asked if you want to continue, enter **Y**.

Step 3 Save your changes by entering this command:
save config

Step 4 Disable the access point radio by entering this command:
config 802.11b disable *Cisco_AP*

Step 5 Configure the access point to scan only the DCA channels supported by its country of operation by entering this command:
config ap monitor-mode tracking-opt *Cisco_AP*

Note To specify the exact channels to be scanned, enter the **config ap monitor-mode tracking-opt** *Cisco_AP* command in *Step 6*.

Note To disable tracking optimization for this access point, enter the **config ap monitor-mode no-optimization** *Cisco_AP* command.

Step 6 After you have entered the command in *Step 5*, you can enter this command to choose up to four specific 802.11b channels to be scanned by the access point:
config ap monitor-mode 802.11b fast-channel *Cisco_AP channel1 channel2 channel3 channel4*

Note In the United States, you can assign any value between 1 and 11 (inclusive) to the *channel* variable. Other countries support additional channels. You must assign at least one channel.

Step 7 Reenable the access point radio by entering this command:
config 802.11b enable *Cisco_AP*

Step 8 Save your changes by entering this command:
save config

Step 9 See a summary of all access points in monitor mode by entering this command:
show ap monitor-mode summary

Configuring Probe Request Forwarding

Information About Configuring Probe Request Forwarding

Probe requests are 802.11 management frames sent by clients to request information about the capabilities of SSIDs. By default, access points forward acknowledged probe requests to the controller for processing. Acknowledged probe requests are probe requests for SSIDs that are supported by the access point. If desired, you can configure access points to forward both acknowledged and unacknowledged probe requests to the controller. The controller can use the information from unacknowledged probe requests to improve the location accuracy.

Configuring Probe Request Forwarding (CLI)

Step 1 Enable or disable the filtering of probe requests forwarded from an access point to the controller by entering this command:
config advanced probe filter {**enable** | **disable**}
If you enable probe filtering, the default filter setting, the access point forwards only acknowledged probe requests to the controller. If you disable probe filtering, the access point forwards both acknowledged and unacknowledged probe requests to the controller.

Step 2 Limit the number of probe requests sent to the controller per client per access point radio in a given interval by entering this command:
config advanced probe limit *num_probes interval*
where

- *num_probes* is the number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.

• *interval* is the probe limit interval (from 100 to 10000 milliseconds).

The default value for *num_probes* is 2 probe requests, and the default value for *interval* is 500 milliseconds.

Step 3 Enter the **save config** command to save your changes.

Step 4 See the probe request forwarding configuration by entering this command:
show advanced probe

Information similar to the following appears:

```
Probe request filtering.........................  Enabled
Probes fwd to controller per client per radio....  2
Probe request rate-limiting interval..........  500 msec
```

Retrieving the Unique Device Identifier on Controllers and Access Points

Information About Retrieving the Unique Device Identifier on Controllers and Access Points

The Unique Device Identifier (UDI) standard uniquely identifies products across all Cisco hardware product families, enabling customers to identify and track Cisco products throughout their business and network operations and to automate their asset management systems. The standard is consistent across all electronic, physical, and standard business communications. The UDI consists of five data elements:

- The orderable product identifier (PID)
- The version of the product identifier (VID)
- The serial number (SN)
- The entity name
- The product description

The UDI is burned into the EEPROM of controllers and lightweight access points at the factory. It can be retrieved through either the GUI or the CLI.

Retrieving the Unique Device Identifier on Controllers and Access Points (GUI)

Step 1 Choose **Controller** > **Inventory** to open the Inventory page.
This page shows the five data elements of the controller UDI.

Step 2 Choose **Wireless** > **Access Points** > **All APs** to open the All APs page.

Step 3 Click the name of the desired access point.

Step 4 Choose the **Inventory** tab to open the All APs > Details for (Inventory) page.
This page shows the inventory information for the access point.

Retrieving the Unique Device Identifier on Controllers and Access Points (CLI)

Use these commands to retrieve the UDI on controllers and access points using the controller CLI:

- **show inventory—**Shows the UDI string of the controller. Information similar to the following appears:

```
...
...
NAME: "Chassis"    , DESCR: "Cisco 5500 Series Wireless LAN Controller"
PID: AIR-CT5508-K9,  VID: V01,  SN: XXXXXXXXXXX
```

- **show inventory ap** *ap_id***—**Shows the UDI string of the access point specified.

Performing a Link Test

Information About Performing a Link Test

A link test is used to determine the quality of the radio link between two devices. Two types of link-test packets are transmitted during a link test: request and response. Any radio receiving a link-test request packet fills in the appropriate text boxes and echoes the packet back to the sender with the response type set.

The radio link quality in the client-to-access point direction can differ from that in the access point-to-client direction due to the asymmetrical distribution of the transmit power and receive sensitivity on both sides. Two types of link tests can be performed: a ping test and a CCX link test.

With the *ping link test*, the controller can test link quality only in the client-to-access point direction. The RF parameters of the ping reply packets received by the access point are polled by the controller to determine the client-to-access point link quality.

With the *CCX link test*, the controller can also test the link quality in the access point-to-client direction. The controller issues link-test requests to the client, and the client records the RF parameters (received signal strength indicator [RSSI], signal-to-noise ratio [SNR], and so on). of the received request packet in the response packet. Both the link-test requestor and responder roles are implemented on the access point and controller. Not only can the access point or controller initiate a link test to a CCX v4 or v5 client, but a CCX v4 or v5 client can initiate a link test to the access point or controller.

The controller shows these link-quality metrics for CCX link tests in both directions (out— access point to client; in— client to access point):

- Signal strength in the form of RSSI (minimum, maximum, and average)
- Signal quality in the form of SNR (minimum, maximum, and average)
- Total number of packets that are retried

- Maximum retry count for a single packet
- Number of lost packets
- Data rate of a successfully transmitted packet

The controller shows this metric regardless of direction:

- Link test request/reply round-trip time (minimum, maximum, and average)

The controller software supports CCX versions 1 through 5. CCX support is enabled automatically for every WLAN on the controller and cannot be disabled. The controller stores the CCX version of the client in its client database and uses it to limit the features for this client. If a client does not support CCXv4 or v5, the controller performs a ping link test on the client. If a client supports CCXv4 or v5, the controller performs a CCX link test on the client. If a client times out during a CCX link test, the controller switches to the ping link test automatically.

Note Follow the instructions in this section to perform a link test using either the GUI or the CLI.

Performing a Link Test (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.

Step 2 Hover your cursor over the blue drop-down arrow for the desired client and choose **LinkTest**. A link test page appears.

Note You can also access this page by clicking the MAC address of the desired client and then clicking the **Link Test** button on the top of the Clients > Detail page.

This page shows the results of the CCX link test.

Note If the client and/or controller does not support CCX v4 or later releases, the controller performs a ping link test on the client instead, and a much more limited link test page appears.

Note The Link Test results of CCX clients when it fails will default to ping test results if the client is reachable.

Step 3 Click **OK** to exit the link test page.

Performing a Link Test (CLI)

Use these commands to run a link test using the controller CLI:

- Run a link test by entering this command:

  linktest *ap_mac*

  When CCX v4 or later releases is enabled on both the controller and the client being tested, information similar to the following appears:

```
CCX Link Test to 00:0d:88:c5:8a:d1.
     Link Test Packets Sent..................................... 20
```

```
Link Test Packets Received.............................. 10
Link Test Packets Lost (Total/AP to Client/Client to AP).... 10/5/5
Link Test Packets round trip time (min/max/average)..... 5ms/20ms/15ms
RSSI at AP (min/max/average)............................. -60dBm/-50dBm/-55dBm

RSSI at Client (min/max/average)......................... -50dBm/-40dBm/-45dBm

SNR at AP (min/max/average).............................. 40dB/30dB/35dB
SNR at Client (min/max/average).......................... 40dB/30dB/35dB
Transmit Retries at AP (Total/Maximum)................... 5/3
Transmit Retries at Client (Total/Maximum)............... 4/2
Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M  108M

Packet Count:   0     0     0    0    0    0   0   0     0     2    0   18     0
Transmit rate:  1M   2M   5.5M   6M   9M  11M 12M 18M   24M   36M  48M  54M  108M

Packet Count:   0     0     0    0    0    0   0   0     0     2    0    8     0
```

When CCX v4 or later releases is not enabled on either the controller or the client being tested, fewer details appear:

```
Ping Link Test to 00:0d:88:c5:8a:d1.
        Link Test Packets Sent..................... 20
        Link Test Packets Received................. 20
        Local Signal Strength...................... -49dBm
        Local Signal to Noise Ratio................ 39dB
```

- Adjust the link-test parameters that are applicable to both the CCX link test and the ping test by entering these commands from configuration mode:

  linktest frame-size *size_of_link-test_frames*

  linktest num-of-frame *number_of_link-test_request_frames_per_test*

Configuring Link Latency

Information About Configuring Link Latency

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to the controller but is especially useful for FlexConnect and OfficeExtend access points, for which the link could be a slow or unreliable WAN connection.

The following are some guidelines for link latency:

- Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to the network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo responses received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Note Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

- The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.
- You can configure link latency for a specific access point using the controller GUI or CLI or for all access points joined to the controller using the CLI.

Restrictions for Link Latency

- Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Configuring Link Latency (GUI)

Step 1 Choose **Wireless > Access Points > All APs** to open the All APs page.

Step 2 Click the name of the access point for which you want to configure link latency.

Step 3 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.

Step 4 Select the **Enable Link Latency** check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 5 Click **Apply** to commit your changes.

Step 6 Click **Save Configuration** to save your changes.

Step 7 When the All APs page reappears, click the name of the access point again.

Step 8 When the All APs > Details for page reappears, choose the **Advanced** tab again. The link latency and data latency results appear below the Enable Link Latency check box:

- **Current—**The current round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Minimum—**Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.
- **Maximum—**Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets or data packets from the access point to the controller and back.

Step 9 To clear the current, minimum, and maximum link latency and data latency statistics on the controller for this access point, click **Reset Link Latency**.

Step 10 After the page refreshes and the All APs > Details for page reappears, choose the **Advanced** tab. The updated statistics appear in the Minimum and Maximum text boxes.

Configuring Link Latency (CLI)

Step 1 Enable or disable link latency for a specific access point or for all access points currently associated to the controller by entering this command:
config ap link-latency {**enable** | **disable**} {*Cisco_AP* | **all**}

The default value is disabled.

Note The **config ap link-latency** {**enable** | **disable**} **all** command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

Step 2 See the link latency results for a specific access point by entering this command:
show ap config general *Cisco_AP*

Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
AP Link Latency.................................. Enabled
 Current Delay................................... 1 ms
 Maximum Delay................................... 1 ms
 Minimum Delay................................... 1 ms
 Last updated (based on AP Up Time)........... 0 days, 05 h 03 m 25 s
```

The output of this command contains the following link latency results:

- **Current Delay—**The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Maximum Delay—**Since link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.
- **Minimum Delay—**Since link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 3 Clear the current, minimum, and maximum link latency statistics on the controller for a specific access point by entering this command:
config ap link-latency reset *Cisco_AP*

Step 4 See the results of the reset by entering this command:
show ap config general *Cisco_AP*

Configuring the TCP MSS

Information About Configuring the TCP MSS

If the client's maximum segment size (MSS) in a Transmission Control Protocol (TCP) three-way handshake is greater than the maximum transmission unit can handle, the client might experience reduced throughput and the fragmentation of packets. To avoid this problem in controller software release 6.0 or later releases, you can specify the MSS for all access points that are joined to the controller or for a specific access point.

When you enable this feature, the access point selects the MSS for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

TCP MSS is supported only on APs that are in local mode or FlexConnect with centrally switched WLANs.

Configuring TCP MSS (GUI)

Step 1 Choose **WIRELESS > Access Points > Global Configuration** to open the Global Configuration page.

Step 2 Under TCP MSS, select the **Global TCP Adjust MSS** check box and set the MSS for all access points that are associated with the controller.

Note The valid range are:

- For IPv4 TCP - between 536 and 1363 bytes.
- For IPv6 TCP - between 1220 and 1331.

Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP .

Configuring TCP MSS (CLI)

Step 1 Enable or disable the TCP MSS on a particular access point or on all access points by entering this command: **config ap tcp-mss-adjust** {**enable**|**disable**} {*Cisco_AP* | *all*} *size*

where the *size* parameter is a value between 536 and 1363 bytes for IPv4 and between 1220 and 1331 for IPv6. The default value varies for different clients.

Note The valid ranges are:

- For IPv4 - Use a value between 536 and 1363 bytes.
- For IPv6 - Use a value between 1220 and 1331 bytes.

Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.

Step 2 Save your changes by entering this command:
save config

Step 3 See the current TCP MSS setting for a particular access point or all access points by entering this command:
show ap tcp-mss-adjust {*Cisco_AP* | **all**}

Information similar to the following appears:

```
AP Name              TCP State  MSS Size
------------------   --------   -------
AP-1140              enabled      536
AP-1240              disabled      -
AP-1130              disabled      -
```

Configuring Power Over Ethernet

Information About Configuring Power over Ethernet

When an access point that has been converted to lightweight mode (such as an AP1131 or AP1242) or a 1250 series access point is powered by a power injector that is connected to a Cisco pre-Intelligent Power Management (pre-IPM) switch, you need to configure Power over Ethernet (PoE), also known as *inline power*.

The dual-radio 1250 series access points can operate in four different modes when powered using PoE:

- 20.0 W (Full Power)—This mode is equivalent to using a power injector or an AC/DC adapter.
- 16.8 W—Both transmitters are used but at reduced power. Legacy data rates are not affected, but the M0 to M15 data rates are reduced in the 2.4-GHz band. Throughput should be minimally impacted because all data rates are still enabled. The range is affected because of the lower transmit power. All receivers remain enabled.
- 15.4 W—Only a single transmitter is enabled. Legacy data rates and M0 to M7 rates are minimally affected. M8 to M15 rates are disabled because they require both transmitters. Throughput is better than that received with legacy access points but less than the 20 and 16.8 W power modes.
- 11.0 W (Low Power)—The access point runs, but both radios are disabled.

The following are some guidelines for Power over Ethernet:

- When a dual-radio 1250 series access point is powered using 15.4-W PoE, it cannot operate at full functionality, which requires 20 W. The access point can operate with dual radios on 15.4-W PoE, but

performance is reduced in terms of throughput and range. If full functionality is required on 15.4 W, you can remove one of the radios from the 1250 series access point chassis or disable it in controller software release 6.0 or later releases so that the other radio can operate in full 802.11n mode. After the access point radio is administratively disabled, the access point must be rebooted for the change to take effect. The access point must also be rebooted after you reenable the radio to put it into reduced throughput mode.

These modes provide the flexibility of running the 1250 series access points with the available wired infrastructure to obtain the desired level of performance. With enhanced PoE switches (such as the Cisco Catalyst 3750-E Series Switches), the 1250 series access points can provide maximum features and functionality with a minimum total cost of ownership. Alternatively, if you decide to power the access point with the existing PoE (802.3af) switches, the access point chooses the appropriate mode of operation based on whether it has one radio or two.

Note For more information about Cisco PoE switches, see http://www.cisco.com/c/en/us/products/switches/epoe.html

The table below shows the maximum transmit power settings for 1250 series access points using PoE.

Table 4: Maximum Transmit Power Settings for 1250 Series Access Points Using PoE

Radio Band	Data Rates	Number of Transmitters	Cyclic Shift Diversity (CSD)	Maximum Transmit Power (dBm)[1]		
				802.3af Mode (15.4 W)	ePoE Power Optimized Mode (16.8 W)	ePoE Mode (20 W)
2.4 GHz	802.11b	1	—	20	20	20
	802.11g	1	—	17	17	17
	802.11n MCS 0-7	1 2	Disabled Enabled (default)	17 Disabled	17 14 (11 per Tx)	17 20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	14 (11 per Tx)	20 (17 per Tx)
5 GHz	802.11a	1	—	17	17	17
	802.11n MCS 0-7	1 2	Disabled Enabled (default)	17 Disabled	17 20 (17 per Tx)	17 20 (17 per Tx)
	802.11n MCS 8-15	2	—	Disabled	20 (17 per Tx)	20 (17 per Tx)

[1] Maximum transmit power varies by channel and according to individual country regulations. See the product documentation for specific details.

- When powered with a non-Cisco standard PoE switch, the 1250 series access point operates under 15.4 Watts. Even if the non-Cisco switch or midspan device is capable of providing higher power, the access point does not operate in enhanced PoE mode.

Configuring Power over Ethernet (GUI)

Step 1 Choose **Wireless** > **Access Points** > **All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the All APs > Details for (Advanced) page.
The PoE Status text box shows the power level at which the access point is operating: High (20 W), Medium (16.8 W), or Medium (15.4 W). This text box is not configurable. The controller auto-detects the access point's power source and displays the power level here.

Note This text box applies only to 1250 series access points that are powered using PoE. There are two other ways to determine if the access point is operating at a lower power level. First, the "Due to low PoE, radio is transmitting at degraded power" message appears under the Tx Power Level Assignment section on the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page. Second, the "PoE Status: degraded operation" message appears in the controller's trap log on the Trap Logs page.

Step 3 Perform one of the following:

- Select the **Pre-standard 802.3af switches** check box if the access point is being powered by a high-power 802.3af Cisco switch. This switch provides more than the traditional 6 Watts of power but do not support the intelligent power management (IPM) feature.
- Unselect the **Pre-standard 802.3af switches** check box if power is being provided by a power injector. This is the default value.

Step 4 Select the **Power Injector State** check box if the attached switch does not support IPM and a power injector is being used. If the attached switch supports IPM, you do not need to select this check box.

Step 5 If you selected the Power Injector State check box in the previous step, the Power Injector Selection and Injector Switch MAC Address parameters appear. The Power Injector Selection parameter enables you to protect your switch port from an accidental overload if the power injector is inadvertently bypassed. Choose one of these options from the drop-down list to specify the desired level of protection:

- **Installed—**This option examines and remembers the MAC address of the currently connected switch port and assumes that a power injector is connected. Choose this option if your network contains older Cisco 6-Watt switches and you want to avoid possible overloads by forcing a double-check of any relocated access points.

  If you want to configure the switch MAC address, enter the MAC address in the Injector Switch MAC Address text box. If you want the access point to find the switch MAC address, leave the Injector Switch MAC Address text box blank.

  Note Each time an access point is relocated, the MAC address of the new switch port fails to match the remembered MAC address, and the access point remains in low-power mode. You must then physically verify the existence of a power injector and reselect this option to cause the new MAC address to be remembered.

- **Override—**This option allows the access point to operate in high-power mode without first verifying a matching MAC address. You can use this option if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The advantage of this option is that if you relocate the access point, it continues to operate in high-power mode without any further configuration. The disadvantage of this option is that if the access point is connected directly to a 6-W switch, an overload occurs.

Step 6 Click **Apply**.

Step 7 If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, follow these steps:

a) Choose **Wireless** > **Access Points** > **Radios** > **802.11a/n** or **802.11b/g/n** to open the 802.11a/n (or 802.11b/g/n) Radios page.
b) Hover your cursor over the blue drop-down arrow for the radio that you want to disable and choose **Configure**.
c) On the 802.11a/n (or 802.11b/g/n) Cisco APs > Configure page, choose **Disable** from the **Admin Status** drop-down list.
d) Click **Apply**.
e) Manually reset the access point in order for the change to take effect.

Step 8 Click **Save Configuration**.

Configuring Power over Ethernet (CLI)

Use these commands to configure and See PoE settings using the controller CLI:

- If your network contains any older Cisco 6-W switches that could be accidentally overloaded if connected directly to a 12-W access point, enter this command:

  config ap power injector enable {*Cisco_AP* | **all**} **installed**

  The access point remembers that a power injector is connected to this particular switch port. If you relocate the access point, you must reissue this command after the presence of a new power injector is verified.

  Note Ensure CDP is enabled before entering this command. Otherwise, this command will fail. See the Configuring the Cisco Discovery Protocol section for information about enabling CDP.

- Remove the safety checks and allow the access point to be connected to any switch port by entering this command:

  config ap power injector enable {*Cisco_AP* | **all**} **override**

  You can use this command if your network does not contain any older Cisco 6-W switches that could be overloaded if connected directly to a 12-W access point. The access point assumes that a power injector is always connected. If you relocate the access point, it continues to assume that a power injector is present.

- If you know the MAC address of the connected switch port and do not want to automatically detect it using the installed option, enter this command:

config ap power injector enable {*Cisco_AP* | **all**} *switch_port_mac_address*

- If you have a dual-radio 1250 series access point and want to disable one of its radios in order to enable the other radio to receive full power, enter this command:

  config {**802.11a** | **802.11b**} **disable** *Cisco_AP*

  Note You must manually reset the access point in order for the change to take effect.

- See the PoE settings for a specific access point by entering this command:

  show ap config general *Cisco_AP*

  Information similar to the following appears:

```
Cisco AP Identifier.............................. 1
Cisco AP Name.................................... AP1
...
PoE Pre-Standard Switch.......................... Enabled
PoE Power Injector MAC Addr...................... Disabled
Power Type/Mode.................................. PoE/Low Power (degraded mode)
...
```

  The Power Type/Mode text box shows “degraded mode” if the access point is not operating at full power.

- See the controller’s trap log by entering this command:

  show traplog

  If the access point is not operating at full power, the trap contains “PoE Status: degraded operation.”

- You can power an access point by a Cisco prestandard 15-W switch with Power over Ethernet (PoE) by entering this command:

  config ap power pre-standard {**enable** | **disable**} {**all** | *Cisco_AP*}

  A Cisco prestandard 15-W switch does not support intelligent power management (IPM) but does have sufficient power for a standard access point. The following Cisco prestandard 15-W switches are available:

  - WS-C3550, WS-C3560, WS-C3750
  - C1880
  - 2600, 2610, 2611, 2621, 2650, 2651
  - 2610XM, 2611XM, 2621XM, 2650XM, 2651XM, 2691
  - 2811, 2821, 2851
  - 3631-telco, 3620, 3640, 3660
  - 3725, 3745
  - 3825, 3845

  The **enable** version of this command is required for full functionality when the access point is powered by a Cisco prestandard 15-W switch. It is safe to use if the access point is powered by either an IPM switch or a power injector or if the access point is not using one of the 15-W switches listed above.

You might need this command if your radio operational status is "Down" when you expect it to be "Up." Enter the **show msglog** command to look for this error message, which indicates a PoE problem:

```
Apr 13 09:08:24.986 spam_lrad.c:2262 LWAPP-3-MSGTAG041: AP 00:14:f1:af:f3:40 is unable
 to
verify sufficient in-line power. Radio slot 0 disabled.
```

Configuring Flashing LEDs

Information About Configuring Flashing LEDs

Controller software enables you to flash the LEDs on an access point in order to locate it. All Cisco IOS lightweight access points support this feature.

Configuring Flashing LEDs (CLI)

Use these commands to configure LED flashing from the privileged EXEC mode of the controller:

1. Configure the LED flash for an AP by entering this command:

   config ap led-state flash {*seconds* | **indefinite** | **disable**} {*Cisco_AP*}

   The valid LED flash duration for the AP is 1 to 3600 seconds. You can also configure the LED to flash indefinitely or to stop flashing the LED.

2. Disable LED flash for an AP after enabling it by entering this command:

   config ap led-state flash disable *Cisco_AP*

   The command disables LED flashing immediately. For example, if you run the previous command (with the *seconds* parameter set to 60 seconds) and then disable LED flashing after only 20 seconds, the access point's LEDs stop flashing immediately.

3. Save your changes by entering this command:

   save config

4. Check the status of LED flash for the AP by entering this command:

   show ap led-flash *Cisco_AP*

   Information similar to the following appears:

```
(Cisco Controller)> show ap led-flash AP1040_46:b9
Led Flash..................................... Enabled for 450 secs, 425 secs left
```

Note The output of these commands is sent only to the controller console, regardless of whether the commands were entered on the console or in a TELNET/SSH CLI session.

Viewing Clients

You can use the controller GUI or CLI to view information about the clients that are associated to the controller's access points.

Viewing Clients (GUI)

Step 1 Choose **Monitor** > **Clients** to open the Clients page.
This page lists all of the clients that are associated to the controller's access points. It provides the following information for each client:

- The MAC address of the client
- The name of the access point to which the client is associated
- The name of the WLAN used by the client
- The type of client (802.11a, 802.11b, 802.11g, or 802.11n)

  Note If the 802.11n client associates to an 802.11a radio that has 802.11n enabled, then the client type shows as 802.11a/n. If the 802.11n client associates to an 802.11b/g radio with 802.11n enabled, then the client type shows as 802.11b/n.

- The status of the client connection
- The authorization status of the client
- The port number of the access point to which the client is associated
- An indication of whether the client is a WGB

  Note If you want to remove or disable a client, hover your cursor over the blue drop-down arrow for that client and choose **Remove** or **Disable**, respectively. If you want to test the connection between the client and the access point, hover your cursor over the blue drop-down arrow for that client and choose **Link Test**.

Step 2 Create a filter to display only clients that meet certain criteria (such as the MAC address, status, or radio type) as follows:

a) Click **Change Filter** to open the **Search Clients** dialog box.
b) Select one or more of the following check boxes to specify the criteria used when displaying clients:

- **MAC Address—**Enter a client MAC address.

  Note When you enable the MAC address filter, the other filters are disabled automatically. When you enable any of the other filters, the MAC address filter is disabled automatically.

- **AP Name—**Enter the name of an access point.
- **WLAN Profile—**Choose one of the available WLAN profiles from the drop-down list.
- **Status—**Select the **Associated**, **Authenticated**, **Excluded**, and/or **Idle** check boxes.
- **Radio Type—**Choose **802.11a**, **802.11b**, **802.11g**, **802.11an**, **802.11bn** or **Mobile**.
- **WGB—**Enter the WGB clients associated to the controller's access points.

c) Click **Apply**. The Current Filter parameter at the top of the Clients page shows the filters that are currently applied.

Note If you want to remove the filters and display the entire client list, click **Clear Filter**.

Step 3 Click the MAC address of the client to view detailed information for a specific client. The Clients > Detail page appears. This page shows the following information:

- The general properties of the client
- The security settings of the client
- The QoS properties of the client
- Client statistics
- The properties of the access point to which the client is associated

Viewing Clients (CLI)

Use these commands to view client information:

- See the clients associated to a specific access point by entering this command:

  show client ap {**802.11a** | **802.11b**} *Cisco_AP*

- See a summary of the clients associated to the controller's access points by entering this command:

  show client summary

- See detailed information for a specific client by entering this command:

  show client detail *client_mac*

- See detailed information of the first eight clients that are in RUN state, associated to the controller's access points by entering this command:

  show client username*username*

Configuring LED States for Access Points

In a wireless LAN network where there are a large number of access points, it is difficult to locate a specific access point associated with the controller. You can configure the controller to set the LED state of an access point so that it blinks and the access point can be located. This configuration can be done in the wireless network on a global as well as per-AP level.

Configuring the LED State for Access Points in a Network Globally (GUI)

Step 1 Choose **Wireless** > **Access Points** > **Global Configuration** to open the **Global Configuration** page.

Step 2 Select the **LED state** check box.

Step 3 Choose **Enable** from the drop-down list adjacent to this check box.

Step 4 Click **Apply**.

Configuring the LED State for Access Point in a Network Globally (CLI)

- Set the LED state for all access points associated with a controller by entering this command: **config ap led-state** {**enable** | **disable**} **all**

Configuring LED State on a Specific Access Point (GUI)

Step 1 Choose **Wireless > Access Points > All APs** and then the name of the desired access point.

Step 2 Choose the **Advanced** tab to open the **All APs > Details for (Advanced)** page.

Step 3 Select the **LED state** check box.

Step 4 Choose **Enable** from the drop-down list adjacent to this text box.

Step 5 Click **Apply**.

Configuring LED State on a Specific Access Point (CLI)

Step 1 Determine the ID of the access point for which you want to configure the LED state by entering this command: **show ap summary**

Step 2 Configure the LED state by entering the following command: **config ap led-state** {**enable** | **disable**} *Cisco_AP*